Unified Communications Using Cisco BE6000

Cisco Validated Design Guide

October 2018

Contents

Preface

Documentation for Cisco Validated Designs

Cisco Preferred Architecture (PA) Design Overview guides help customers and sales teams select the appropriate architecture based on an organization's business requirements; understand the products that are used within the architecture; and obtain general design best practices. These guides support sales processes.

Cisco Validated Design (CVD) guides provide detailed steps for deploying the Cisco Preferred Architectures. These guides support planning, design, and implementation of the Preferred Architectures.

Cisco Collaboration Solution Reference Network Design (SRND) guides provide detailed design options for Cisco Collaboration. The SRND should be referenced when design requirements are outside the scope of Cisco Preferred Architectures.

Related PA Guides

Preferred Architecture for Cisco Collaboration 12.0 On-Premises Deployments, Design Overview

Related CVD Guides

Collaboration Edge Using Cisco Business Edition 6000

To view the related CVD guides, click the titles or visit the following site: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/PAdocs.html

Scope

Organizations require high-quality voice and video communications that can scale up to a thousand users using Cisco Business Edition 6000 (BE6000). They need a solution that is easy to deploy and simple to manage from a central location, without replicating costly features at their remote sites.

This document details **Centralized Unified Communications**. It covers the following areas of technology and products:

- Unified Communications applications, such as IP telephony Voicemail and IM and Presence
- Virtualized servers
- Voice gateways and conference bridges
- IP telephones with remote-site survivability
- Session Initiation Protocol (SIP) signaling
- Lightweight Directory Access Protocol integration
- Cisco Prime Collaboration Provisioning (PCP)

For more information, see the *Design Overview* section.

Proficiency

This guide is for people with technical proficiencies—or equivalent experience in CCNA Collaboration—1 to 3 years in designing, installing, and troubleshooting voice and unified communications applications, devices, and networks.

Comments and Questions

If you would like to comment on a guide or ask questions, please email collab-mm-cvd@external.cisco.com.

Disclaimer

The IP address scheme used in this document is for representational purposes only.

Introduction

Communication is the lifeblood of an organization, and in today's global economy, the desire to stay in touch in many different ways has never been greater. The methods people have used to collaborate have changed over the years, but the ability to work seamlessly with others has always been very important to the success of a business.

To remain competitive, you need to provide reliable and consistent access to your communications resources. The importance of dependable collaboration channels inside and outside of your organization cannot be overstated. To be effective, collaboration technology must be easy to deploy and manage, and intuitive to use.

Technology Use Case

Collaboration has always been an essential component of a successful organization. New pressures, heightened by a challenging global economic environment, are making organizations realize collaboration is more important than ever. Specifically, they are trying to manage operational expenses and capital expenses while increasing worker productivity and staying ahead of the competition.

You can accomplish this *do more with less* approach only if you:

- Empower your workforce—Users are empowered when they have communication tools at their disposal that allow them to access and use information when they need it most. Younger employees—especially those of the "Generation Y" demographic, who are now in their twenties—are bringing these networking tools into the workplace. Organizations need to develop a concerted strategy to proactively manage these technologies, and ideally, develop organizational capabilities to take the best advantage of them.
- Provide real-time communication—Collaborative applications enable real-time communication to empower users and provide better information sharing and privacy. As information is shared across the entire user community, its accuracy is more easily verified and corrected.
- Accelerate through innovation—Organizations that successfully adopt new collaborative processes are able to move faster, make better decisions, draw from a deeper base of information, and effectively operate across time and distance barriers. As is always the case in business, either you pull ahead, or the competition will leave you behind.

The challenges are addressed with collaboration services, such as web-conferencing applications, unified communications, and video-collaboration meetings. However, providing these types of capabilities to an entire organization requires a robust and scalable network infrastructure.

Use Case: Centralized Unified Communications

Organizations require high-quality voice and video communications that can scale to a thousand users. They need a solution that is fast to deploy and easy to manage from a central location, without replicating costly features at their remote sites.

This design guide explains how to deploy the following capabilities:

- Single cluster centralized design—Makes the solution simpler to deploy, and easier to manage from a centralized site, to save on infrastructure components. In the single cluster centralized design, each remote site connects to the headquarters site through a WAN, and each site receives call processing features from the headquarters location.
- Self Provisioning—Enables an end user or an administrator to add an unprovisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort.
- Lightweight Directory Access Protocol integration—Uses LDAP directory integration with Prime Collaboration Provisioning(PCP) for designs that require a single source of information for user management.
- Dial Plan—Enables you to control how Public Switched Telephony Network (PSTN) is handled for your users. Site or country-specific dialling behaviors may be added using Prime Collaboration Provisioning.
- Uniform on-net dial plan—Uses endpoint addressing that consists of a uniform on-net dial plan containing 4-digit extensions. An optional access code and 2-digit or 3-digit site codes are available with local site 4-digit dialing.
- Local route groups—Uses local route groups to reduce the number of route patterns required to provision Session Initiation Protocol (SIP) gateways for all sites.
- Class of service—Provisions class of service (CoS) categories with the use of partitions and calling search spaces to enable emergency, local, long distance, and international dialing capabilities.
- Survivable Remote Site Telephony (SRST)—Provides failover at each remote site by standard SRST for SIP and Skinny Client Control Protocol (SCCP) phones.
- Device Mobility—Uses the Device Mobility feature, which enables Cisco Unified CM to determine the physical locations of devices and apply call handling policies accordingly.
- Server load balancing—Load-balances phones across Cisco Unified CM redundancy groups on a phone-by-phone basis.
- Extension Mobility—Uses the Cisco Extension Mobility feature for all phones, which enables users to assign a Cisco Unified IP Phone as their own or move from phone-to-phone within the organization.
- Media resources—Provisions individual media resources, such as conference bridges, for every site.
- Call Admission Control—Provides location-based Call Admission Control (CAC) for a typical hub-and-spoke WAN environment.
- Voice messaging—Provisions Cisco Unified CM for voice messaging integration and configured with Prime Collaboration Provisioning(PCP).
- Instant Messaging and Presence—Provisions Cisco Unified CM IM and Presence service integration.
- Point-to-Point Video—Enables automatic point-to-point video calling between two participants with video endpoints.
- Simplified Administration—Cisco Prime Collaboration Provisioning provides simplified and unified management for multiple services from a single interface.

Design Overview

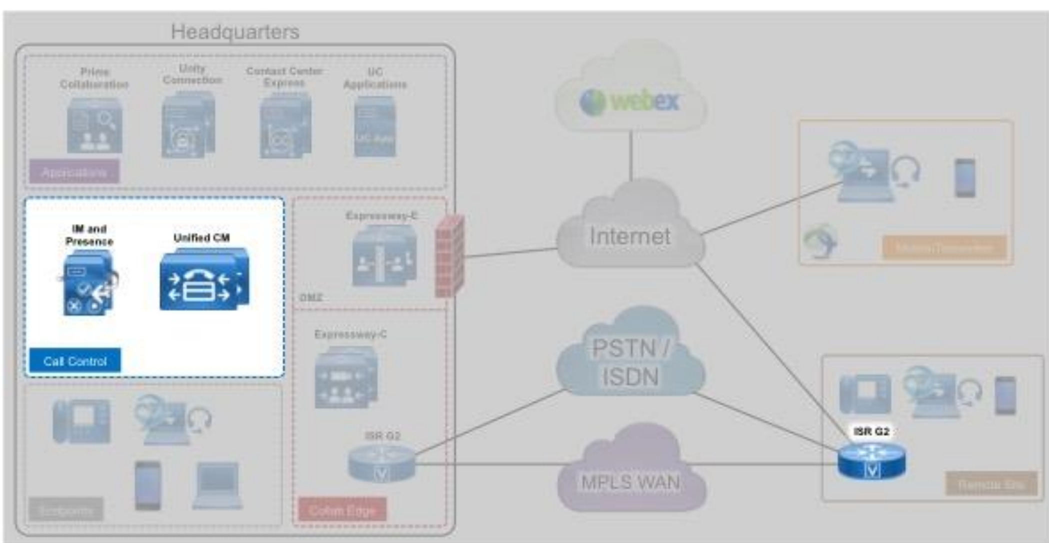
This design guide reduces cost of technology selection and implementation by recommending appropriate equipment and using methods and procedures that have been developed and tested by Cisco. Applying the guidance in this document reduces the time required for adoption of the technology and enables the components to be deployed quickly, accurately, and consistently so that you can achieve a headstart in realizing the return on investment.

IP telephony as a technology is the migration of the old standalone phone switch to a software-based switch, where the data network becomes the physical transport for voice communications, rather than using separate cabling plants for data and voice communications. The market category that defines IP telephony and other forms of voice and video communications is known as unified communications.

Cisco Preferred Architecture

Cisco Preferred Architectures (PAs) provide recommended deployment models for specific market segments based on common use cases. They incorporate a subset of products from the Cisco Collaboration portfolio that is best suited for the targeted market segment and defined use cases. These deployment models are prescriptive and built to scale with an organization as its business needs change. This prescriptive approach simplifies the integration of multiple system-level components and enables an organization to select the deployment model that best addresses its business needs.

The Cisco Preferred Architecture (PA) recommends capabilities that enable organizations to realize immediate gains in productivity and add value to their current voice deployments.



Solution Details

The Unified Communications CVD includes the following components:

- Cisco Unified Communications Manager (Unified CM) for call control and SIP endpoint registrations.
- Cisco Unity Connection for voice messaging.
- Cisco Unified CM IM & Presence for instant messaging and to show presence status for endpoints.
- Cisco Prime Collaboration Provisioning for provisioning endpoints and integrating UC applications.
- Desktop (Cisco 8800 Series IP phones, Cisco Jabber and Cisco Desktop Collaboration Experience DX Series) and multipurpose (Cisco TelePresence SX 10, Webex Room Kit) systems for placing and receiving calls.

Cisco Unified Communications

The products and priorities for this design are based on requirements from customers, partners, and Cisco field personnel. Your specific business requirements may be different from those in this guide, in which case, the product selection may not exactly match your needs.

Cisco Unified Communications has the following software components:

- Cisco Unified CM provides the Internet Protocol private branch exchange (IP PBX) functionality for all users within the headquarters site and the remote sites. The first Unified CM appliance is known as the publisher because it contains the master database to which all other Unified CM appliances within the same cluster subscribe. The rest of the appliances are known as either *subscribers* or *Trivial File Transfer Protocol (TFTP) servers*, based on their function in the cluster.
- Cisco Unity Connection provides voicemail services, voicemail integration with your email inbox, and many other productivity features. Voicemail is considered part of the unified communications foundation.
- Cisco IM and Presence provides personal and group instant messaging services, and presence information to users.

This guide uses a 1:1 publisher-subscriber cluster design to provide redundant call control for the target use case.

Single Cluster Centralized Design

The following single cluster centralized design model provides a highly available and scalable call-control and voicemail system capable of unified messaging.

The Cisco Business Edition (BE) 6000 uses a single Cisco UCS server platform for up to 1000 users. The virtualized server provides the following:

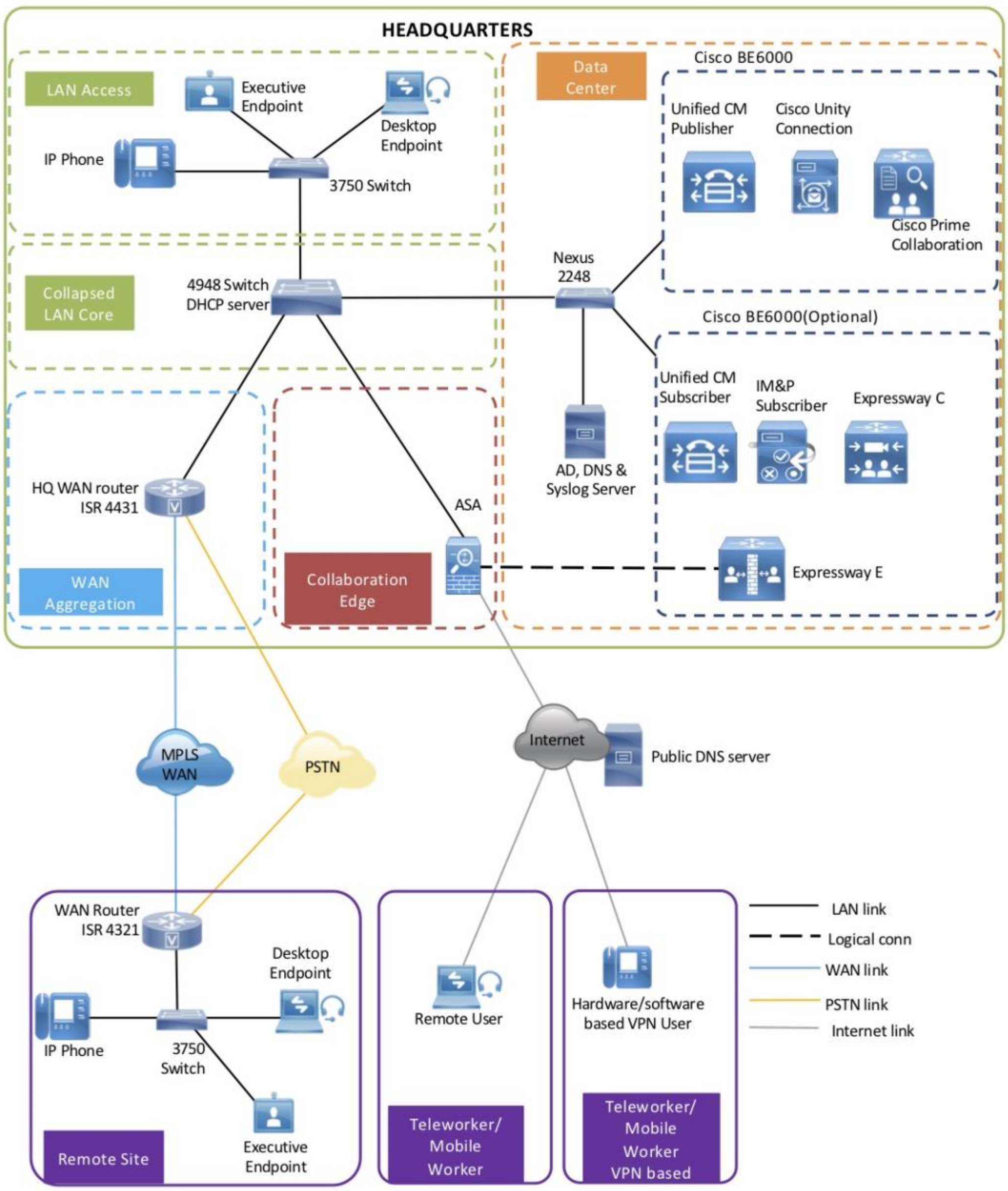
- The publisher, subscriber and TFTP functions are combined with Cisco Unity Connection on a single hardware platform in order to help lower the capital and operational expenses.
- The Cisco UCS C220 M5 hardware platform for the BE6000 is a 1-rack-unit form factor.

- The Cisco Business Edition 6000 supports Cisco Instant Messaging and Presence and Cisco Unified Contact Center Express on the same virtual server platform. You can also add a redundant server to this configuration if an organization requires it.

For the design model, the following features are provided:

- Connection of each server to a different switch within the server room or data center to provide high availability, should a switch or link connection fail.
- Sufficient capacity for multiple devices for each user. For example, you can enable a desk phone and a soft phone with enough computer telephony integration to allow a high percentage of users to have click-to-call or other applications that can remotely control their phones.
- Additional capacity is available for phones that are not assigned to a specific user, such as those in public areas, meeting rooms, storage areas, and break rooms.
- Cisco Unity Connection is deployed as a simple voicemail system. However, with additional configuration, it will provide calendar-based call handling, integration with Microsoft Exchange, and other networkable voicemail systems. Cisco Unity Connection is deployed in the architecture as non-redundant, although a second high-availability server can be added, if required.
- Support for other services, including conferencing, contact center, video conferencing and Collaboration Edge. These advanced services are discussed in other design guides.

Network Block diagram with Cisco Unified CM, Cisco Unity Connection, and Unified CM IM and P



The centralized design consists of a headquarters site and up to 49 remote sites. The Cisco Unified CM and the Cisco Unity Connection server instances are placed at the main site to handle the call processing for up to 1000 telephony users with voice messaging and Cisco Prime Collaboration Provisioning (PCP). An optional BE6000 server can be placed at the main site for redundancy and to install other applications. Each remote site takes advantage of a Cisco ISR 4000 router that was deployed as part of the WAN deployment. Remote worker/mobile worker use cases leveraging Cisco Expressway C and Expressway E are discussed in detail in Collab Edge using BE6000 Design Guide.

Cisco Unified Computing System

Cisco Unified Communications applications, such as IP telephony and voicemail, have different processing and storage requirements based on the number of users and the features applied, therefore it is important to select the appropriate server platform based on the expected usage.

For 1000 users or fewer, Cisco Business Edition (BE) 6000 is recommended. A second BE6000 server may be added for organizations that require hardware redundancy.

Cisco Prime Collaboration Assurance and Analytics–Business

Cisco Prime Collaboration Assurance and Analytics—Business is a monitoring and data analytics management application system. It provides complete service assurance by monitoring the availability and performance of Unified Communications Manager applications, Cisco Gateways, and Cisco UCS (C-series) hardware running in the network. Cisco Prime Collaboration Assurance and Analytics—Business detects hardware failures and performance degradation, analyzes and reports on asset usage, call traffic, service quality experience, and capacity of shared resources such as Time Division Multiplexing (TDM)/Session Initiation Protocol (SIP) trunks, and gateway Digital Signal Processor (DSP).

Cisco Prime Collaboration Assurance and Analytics—Business can monitor up to two Unified Communications Manager and two Expressway clusters.

Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration Provisioning (PCP) provides a scalable web-based solution to manage a company's next-generation communication services. Prime Collaboration Provisioning manages IP communication endpoints and services in an integrated IP telephony, video, voicemail, and unified messaging environment. This environment includes Cisco Unified Communications Manager, Cisco UCM Instant Messaging and Presence, Cisco Unity, Cisco Unity Connection systems, and Analog Gateways.

Self Provisioning

The Self-Provisioning feature enables an end user or administrator to add an unprovisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort. A phone can be added by plugging it into the network and following a few prompts to identify the user. This feature enhances the out-of-box experience for end users by allowing them to directly add their desk phone or soft client without contacting the administrator. It simplifies administrator deployments by allowing them to add desk phones on behalf of an end user. The feature lets administrators and users deploy a large number of devices without interacting directly with the Cisco Unified Communications Manager Administration GUI, but from the devices themselves. The feature relies on the administrator preconfiguring a number of templates and profiles, so that when the phone attempts to self-provision, the necessary information is available in the system for it to create a new device.

Active Directory Integration

Active Directory integration enables you to provision users automatically from the corporate directory into the Cisco Prime Collaboration Provisioning database, which makes it possible to maintain a single directory as opposed to separate directories. Therefore, you don't have to add, remove, or modify core user information manually in PCP each time a change occurs in the corporate directory. The other advantage is that end users are able to authenticate to PCP by using the same credentials in Active Directory, which reduces the number of passwords across the network.

Cisco Voice Gateways

Cisco Integrated Services Routers (ISR) provide gateway services to public telephone networks, audio conferencing resources, resilient call control for remote sites. The combination of these voice services in a single platform offers savings over the individual components. The voice services can be provided by an ISR that also connects to the wide area data network, or they can be deployed in a standalone ISR for additional capacity and redundancy.

The decision to integrate voice into an existing ISR depends on required voice capacity and the overall performance of the model. If an ISR is consistently running above 40% CPU, voice services are better suited for a dedicated system in order to avoid processing delays for voice traffic. If the ISR has limited slots available for voice interface cards or digital signal processors, a dedicated system is recommended to allow additional capacity when needed. ISRs used for voice services at the headquarters location are connected to the datacenter or server room switches. At a remote location, they are connected to the access or distribution switches.

The sizing information in this guide supersedes the information from the various CVD WAN design guides because the number of SRST users determines the proper router model, as listed in the following table.

Table 1. Standalone Voice Gateway Scaling Options

	Voice gateway	Voice T1/E1	Trunk ports
50 users	Cisco 4321	8	240
100 users	Cisco 4331	12	360
1200 users	Cisco 4431	24	720

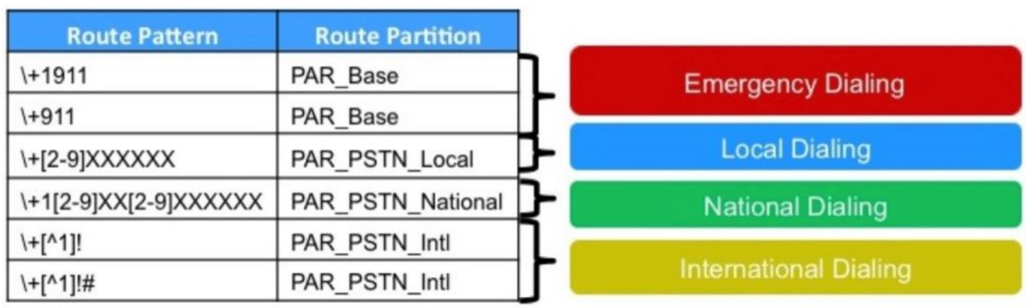
Dial Plan

The dial plan is one of the key elements of an IP telephony system and an integral part of all call-processing agents. Generally, the dial plan is responsible for instructing the call-processing agent on how to route calls. PCP configures a +E.164 dial plan as part of the path selection for PSTN destinations. You can modify the dial plan to meet your specific needs. Cisco recommends using the E.164 dial plans as shown in the examples below.

	Reader Tip

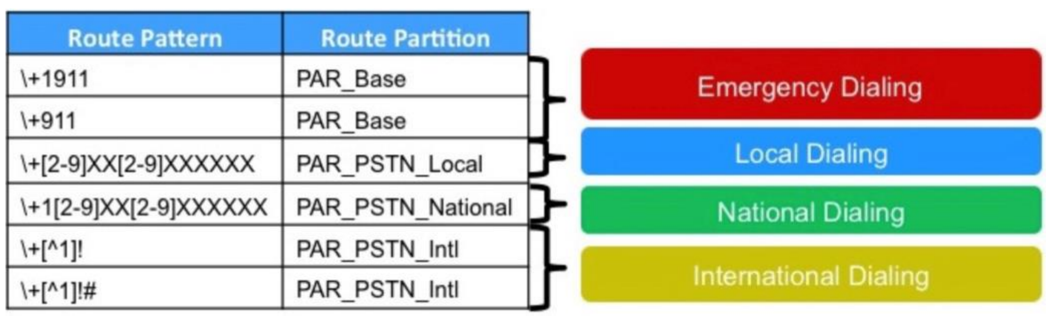
PCP can be used to deploy the default templates and to create new dial plans or to modify the existing ones.

Figure 1. +E.164 dialing for NANP with seven digit local dialing



Route Pattern	Route Partition
\+1911	PAR_Base
\+911	PAR_Base
\+[2-9]XXXXXX	PAR_PSTN_Local
\+1[2-9]XX[2-9]XXXXXX	PAR_PSTN_National
\+[^1]!	PAR_PSTN_Intl
\+[^1]!#	PAR_PSTN_Intl

Figure 2. +E.164 dialing for NANP with ten digit local dialing

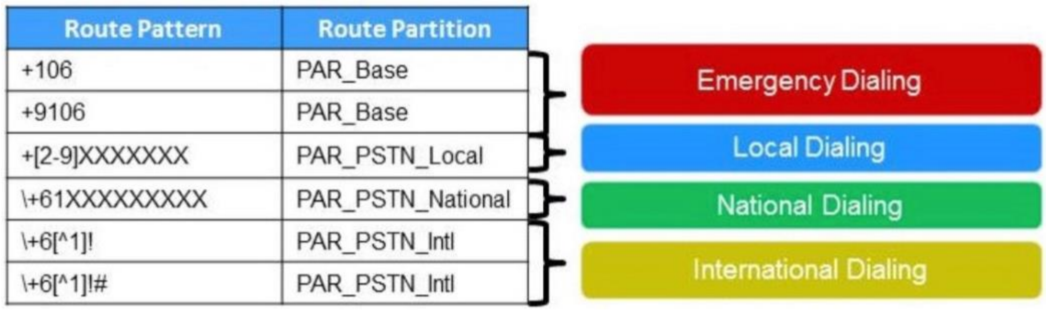


Route Pattern	Route Partition
\+1911	PAR_Base
\+911	PAR_Base
\+[2-9]XX[2-9]XXXXXX	PAR_PSTN_Local
\+1[2-9]XX[2-9]XXXXXX	PAR_PSTN_National
\+[^1]!	PAR_PSTN_Intl
\+[^1]!#	PAR_PSTN_Intl

There are two configured international route patterns: one to route the variable-length dialed digits and one configured with a pound symbol (octothorpe) to allow users to bypass the inter-digit timeout. The +911 and +1911 emergency route patterns are created with urgent priority to prevent inter-digit timeout delays when they are entered from a phone.

Dial plans can be configured using PCP to suit any country. For example, for an Australian dial plan the table below shows some route patterns and their respective route partitions.

Figure 3. +E.164 dialing for Australia



Route Pattern	Route Partition
+106	PAR_Base
+9106	PAR_Base
+[2-9]XXXXXXX	PAR_PSTN_Local
\+61XXXXXXXXX	PAR_PSTN_National
\+6[^1]!	PAR_PSTN_Intl
\+6[^1]!#	PAR_PSTN_Intl

Site Codes

It is recommended that you use a uniform on-net dial plan containing an access code, a site code, and a four-digit extension. The use of access and site codes enables the on-net dial plan to differentiate between extensions at remote sites that could otherwise overlap with each other.

When you use this method, a phone in San Jose, CA can have the same four-digit extension as one in Houston, TX without creating a numbering conflict. For example: 408-555-1234 in San Jose and 713-555-1234 in Houston.

For networks with up to 50 sites, the dial plan consists of the following:

- One digit as an inter-site access code
- Two digits for the site code
- Four digits for the site extension

Cisco recommends a format of 8 + SS + XXXX, where 8 is the on-net access code, SS is a two-digit site code of 10-99, and XXXX is a four-digit extension number, giving a total of seven digits.

Figure 4. Two-digit Site Code Format

Class of Service

Class of Service (CoS) is configured in Cisco Unified CM by using calling search spaces and partitions. There are four classes of service defined in this guide, and they provide PSTN access for emergency, local, national, and international dialing.

Figure 5. Calling Search Spaces and Partitions

	Calling Search Space	Route Partition 1	Route Partition 2	Route Partition 3
1	CSS_Base	PAR_Base	—	—
2	CSS_LocalPSTN	PAR_PSTN_Local	—	—
3	CSS_NationalPSTN	PAR_PSTN_Local	PAR_PSTN_National	—
4	CSS_InternationalPSTN	PAR_PSTN_Local	PAR_PSTN_National	PAR_PSTN_Intl

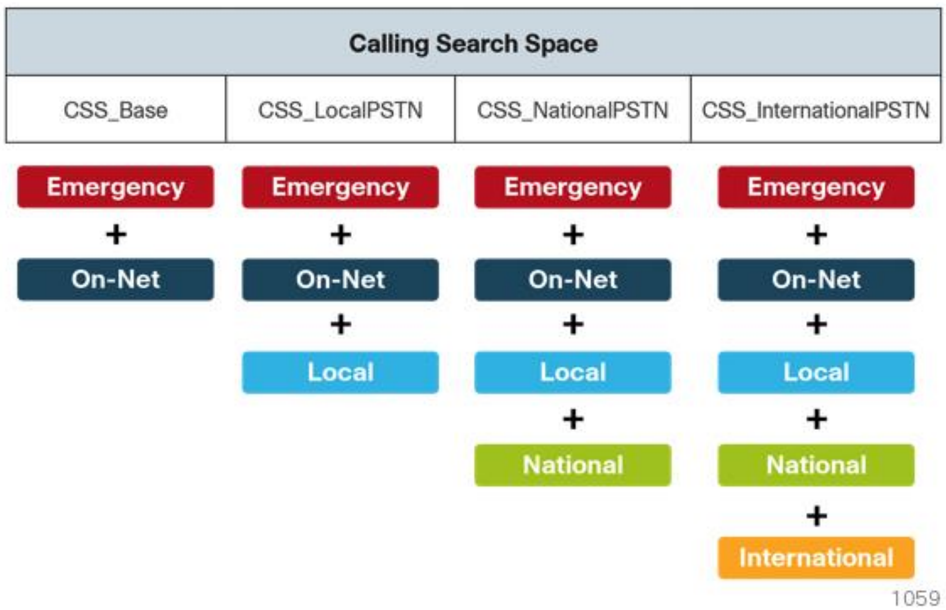
1 Emergency Dialing
2 Local Dialing
3 National Dialing
4 International Dialing

1058

Using PCP's Getting Started Wizard (GSW), if administrators choose the default CSS that is defined, the auto registration partition will default to CSS_Base. This enables all devices to dial both on-net and emergency off-net numbers.

The remaining calling search spaces are configured on the user device profile directory number and provide local seven-digit or local ten-digit, national, and international dialing capabilities.

Figure 6. Calling Capabilities for Calling Search Spaces



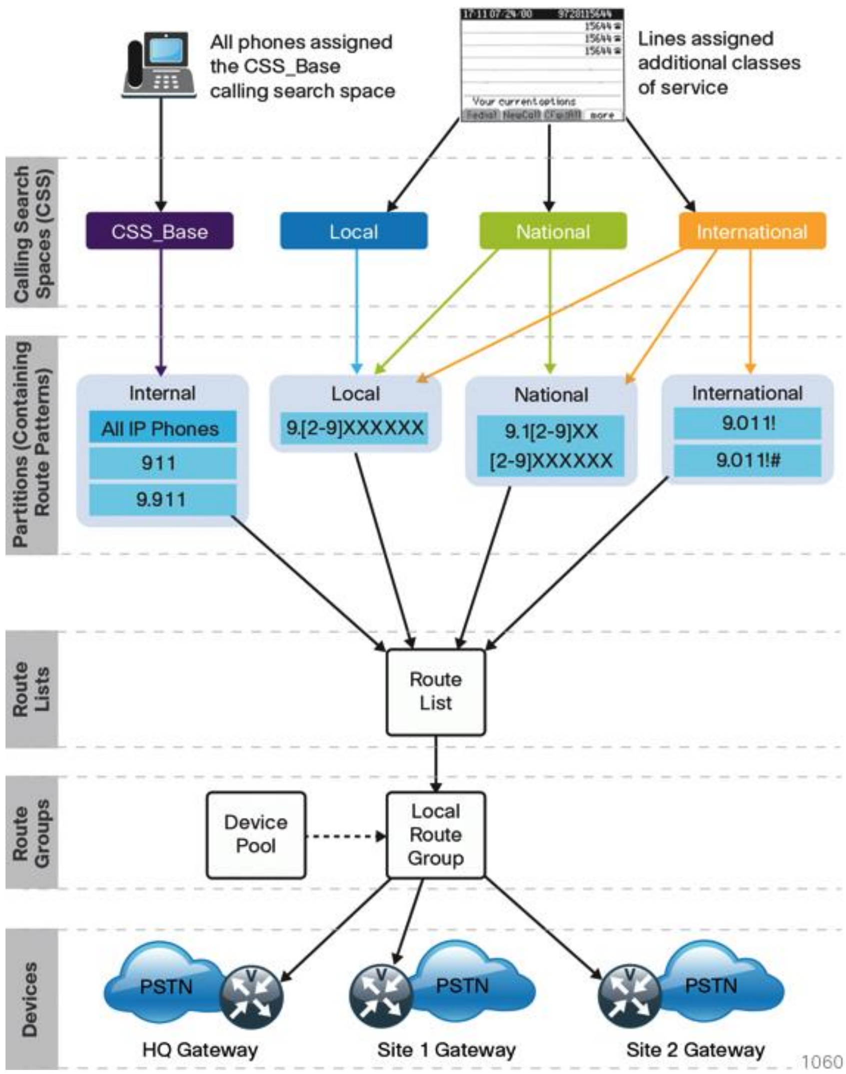
For example, if a user requires international dialing capability, their directory number would be assigned the CSS_InternationalPSTN calling search space, which includes dialing accessibility to all PSTN route patterns and national, local, emergency, and on-net numbers.

Local Route Groups

The Local Route Group feature in Cisco Unified CM decouples the PSTN gateway physical location from the route patterns and route lists that are used to access the gateway. The feature assigns a local route group to each route group, based on the device pool setting of the originating device. Therefore, phones and other devices from different locations can use a single set of route patterns, but Unified CM selects the correct gateway to route the call.

PCP assigns a unique route group to a device pool so each site can choose the correct SIP gateway. The route group is associated with the device pool by using the local route group setting. This simplifies the process of provisioning by allowing the administrator to create a single set of route patterns for all sites. When a call is made from a device that matches the route pattern, Cisco Unified CM uses the Local Route Group device pool setting to determine the proper route group, which selects the SIP gateway assigned to the site.

Figure 7. Cisco Unified CM Call Routing



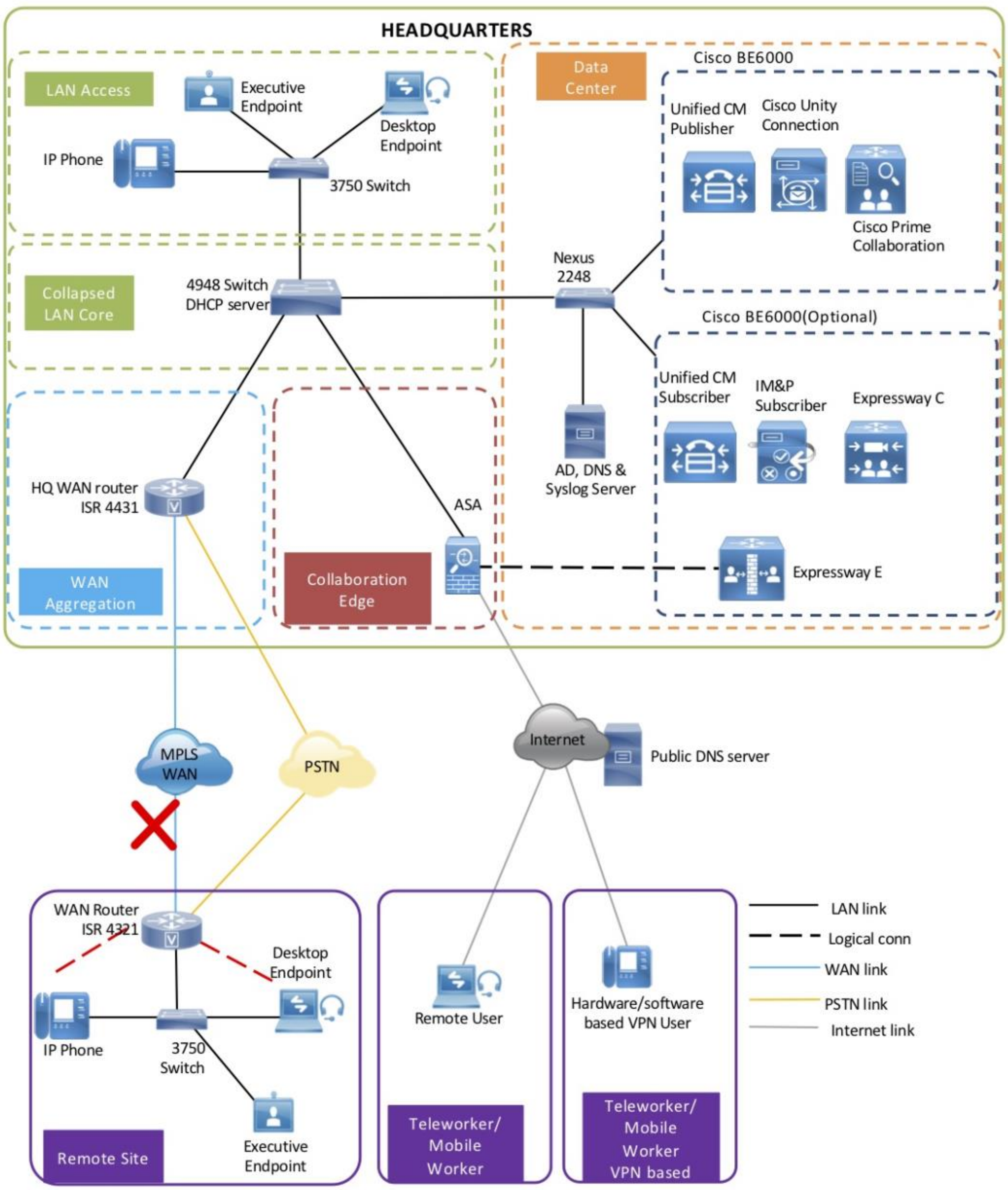
Survivable Remote Site Telephony

In a centralized design, when IP phones lose connectivity to Cisco Unified CM because the application is unreachable, IP phones in remote-site offices or teleworker homes lose call processing capabilities. The Survivable Remote Site Telephony (SRST) feature provides basic IP telephony backup services because IP phones fall back to the local router at the remote site when connectivity is lost. IP phones continue to make calls within the site and out the local gateway to the PSTN.

At a remote site with more than one PSTN gateway, configure SRST on the router with the most voice ports. If only one router has PSTN interfaces, SRST must be configured on the router to reduce complexity.

The following diagram shows SRST providing service to phones at a remote site when the WAN is down.

Figure 8. SRST at a Remote Site



When a remote site falls back to SRST and site codes are in use, voice translation commands are required in the router to maintain four-digit local dialing. The commands are explained in more detail in the deployment section of this guide.

The Forward on No Registration feature enables the calls to the remote site through the PSTN, in the event of a call failure.

Device Mobility

PCP uses *device mobility* that enables Cisco Unified CM to determine if the IP phone is at its home or a roaming location. Unified CM uses the device's IP subnet to determine the physical location of the IP phone. By enabling device mobility within a cluster, mobile users can roam from one site to another, thus acquiring the site-specific settings. Unified CM then uses these dynamically allocated settings for call routing, codec selection, media resource selection, and Unified CM groups.

This feature is used primarily to reduce the configuration on the devices themselves by allowing configuration of many parameters at the site level. These parameters are dynamically applied, based on the subnet to which the device is attached. This enables a fast and reliable deployment because the administrator does not have to configure each phone individually or ensure the phone is at the correct location.

Extension Mobility

Extension Mobility enables end users to personalize a Cisco Unified IP Phone temporarily. The Extension Mobility feature dynamically configures a phone according to the authenticated user's device profile. Users log into an IP phone with their username and PIN, and their device profile is uploaded to the IP phone. Extension Mobility alleviates the need for device-to-user association during provisioning. This saves deployment time while simultaneously allowing the user to log into any phone within the organization, allowing phone-sharing capabilities.

Extension Mobility can be enabled in such a way that it enables users to log into IP phones but does not allow them to log out. With this method, Extension Mobility is exclusively designed for IP phone deployment, but not as an ongoing feature in the organization. Extension mobility can be used for hot desking and enables a user to move between floors, sites, or geographic locations, and utilize an available Cisco IP phone.

Media Resources

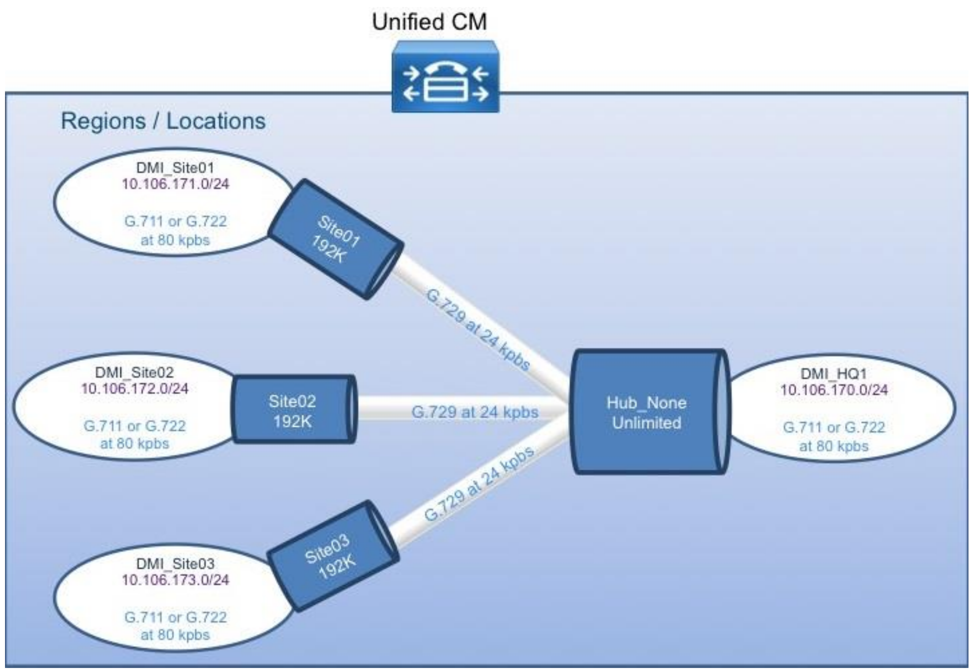
Media resources have been provisioned as part of the procedure for every site in order to ensure that remote sites use their local conference bridges and avoid unnecessary voice traffic over the WAN. The names of the conference bridges need to match those provisioned by PCP. The names are always CFB1<*Site Name*> and CFB2<*Site name*>, if there are two. For example, if the headquarters site is HQ1, the conference bridge names are CFB1HQ1 and CFB2HQ1.

Call Admission Control

The default design is a hub-and-spoke topology in which each remote site is connected to the headquarters site over a bandwidth-constrained WAN. The PCP design uses regions and locations to define locations-based Call Admission Control. For calls within a site, the regions are configured for the G.722 or G.711 codec running at 80 kbps, and there are no limits to the number of calls allowed within a site. For calls between the sites, the regions are configured for the G.729 codec running at 24 kbps.

By default, Call Admission Control is not calculated for calls to and from the central site (headquarters). It's expected that as long as the spokes are provisioned for Call Admission Control, the hub will not be oversubscribed on a traditional WAN. This is the case for all hub-and-spoke topologies; however, for a Multiprotocol Label Switching (MPLS)–based network, which is considered a hub-less hub and spoke, you will need to modify the headquarters site default bandwidth to provide the correct Call Admission Control based on the speed of the link.

Figure 9. Hub-and-spoke Topology for Call Admission Control



Point-to-Point Video

PCP can be used to deploy all the video models, including the DX devices.

IM and Presence

Cisco Jabber for Windows streamlines communications and enhances productivity by unifying presence, instant messaging, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one desktop client. It offers flexible deployment models and integrates with commonly used applications. Cisco Jabber for Windows can also be deployed in virtual environments. In a virtual environment, it supports presence, instant messaging, and desk-phone control.

Cisco Jabber solutions can be deployed using a mixture of on-premises and cloud-based solutions.

The on-premises Jabber solution includes the following components:

- Unified CM IM and Presence for instant messaging and presence

- Unified CM for audio and video call management, user and device configuration, and Jabber software phone and directory synchronization
- Cisco Unity Connection for voice mail
- Jabber for Windows, Jabber for Mac, Jabber for iPad, Jabber for iPhone, and Jabber for Android
- Microsoft Active Directory for client user information
- WebEx Meeting Center for hosted meetings
- Network Time Protocol (NTP) server for logging consistency
- Domain Name System (DNS) server for name-to-IP resolution
- Syslog server for logging events (optional)

This guide describes the following Cisco Jabber features:

- Communication integration—Use a single, intuitive interface for instant messaging with individuals and groups. Includes IP telephony, visual voicemail, voice and web conferencing, desktop sharing, communication history, and integrated directories.
- Presence—View real-time availability of co-workers and colleagues within and outside the enterprise network.
- Enterprise instant messaging—Chat in real time by using instant messaging. Several chat modes are supported, including:
    - Point-to-point chat with co-workers inside your network, or supported federated business and personal contacts
    - Group chat, which enables multiple colleagues to communicate and collaborate in a single discussion
    - Personal instant messaging history for your reference
- Predictive search—Provides suggestions to you as you type in a search query and is capable of indexing your Cisco Jabber contact list, recent contacts, Microsoft Active Directory, or LDAP directory.
    - Media escalation—Escalate from a chat to an audio call, video call, desktop share, or web meeting. Media escalations are as easy as clicking a button.
    - Desktop share—Share what is on your desktop with Cisco Jabber users, as well as Cisco and other standards-based video endpoints.
    - Integrated voice and video telephony—A coordinated video display on the screen and voice conversation with a dedicated soft phone.

      You can make, receive, and control your phone calls whether you are in or out of the office and support business-quality video communication up to high-definition (720p) and high-fidelity wideband audio. You can also use voice, video, and even desktop sharing when interacting with TelePresence endpoints and room-based and multipoint videoconferencing systems.

      Many call control options are available, including mute, call transfer, call forwarding, and ad-hoc conferencing. The reliability and failover features of Cisco Unified Communications Manager are supported.

- Visual voice message access—Access and manage your voice messages.
    - View, play back, and delete voice messages from Cisco Unity Connection.
    - Secure messaging is provided, with support for private and encrypted voice messages.

Self Care

Unified Communications Self Care Portal is used to configure user settings for your Cisco Unified IP Phones and Jabber applications. Using Unified Communications Self Care Portal, end users can configure settings such as speed dial numbers, contact lists, phone services, and voicemail notifications. The administrator can control user access to the Self Care portal. Before a user can start using the Self Care portal, they should be added as a user to the Cisco Unified Communications Manager end user group. The URL to access the Self Care portal is https://cucmhostname:portnumner/ucmuser.

Phone Models

For decades, traditional phone systems have provided basic dial tone and voicemail services, but there is little they can offer in terms of advanced communication features. Organizations who lead the way in technological innovation expect the next generation of handsets to provide features that will transform the way they operate their business. Even as they lead the way with new tools and technology, they want to cut costs by eliminating expensive wiring to every desktop and lowering electricity usage. The high cost of energy and the push for a greener planet is causing organizations to rethink every aspect of their business to see if they can lower their carbon footprint.

Cisco Unified IP Phone 7800 Series is a high-fidelity voice communications portfolio designed for people- centric collaboration. It combines always-on reliability and security, full-featured easy-to-use IP telephony, and wideband audio to increase productivity, with an earth-friendly design for reduced costs. These basic phone models provide essential calling functionality and still maintain the inherent flexibility of an IP-based endpoint, which operates from an existing Ethernet port for power and connectivity. The Cisco IP Phone 7800 Series brings a higher quality standard, with full wideband audio support for handset, headset and speaker, to our voice-centric portfolio. A new ergonomic design includes support for larger grayscale, graphical backlit displays.

Cisco Unified IP Phone 7821 is a two-line, endpoint that is designed for information workers and managers. The Cisco IP phone 7841 is a four-line endpoint that is designed for information workers, the administrative staff and managers who have a moderate level of voice communication needs. The Cisco IP phone 7861 has 16 lines and is ideal for users such as administrative staff, managers and agents in contact centers.

Cisco Unified IP Conference Phone 8831 is recommended for conference rooms, and the Cisco IP Communicator software client is recommended to provide a desktop computer solution.

The 8800 Series are the best audio-performing IP phones Cisco has ever delivered. Wideband (G.722) audio is supported on all models and the 8811, 8841,8845, 8851, 8861, and 8865 desk endpoints are hardware-enhanced for higher performance on echo cancellation. In addition, vibration isolation of the hardware has been applied to both speakers and microphones, resulting in a higher-quality communications experience.

With Cisco Intelligent Proximity for Mobile Voice, Cisco is bringing the worlds of desktop and mobile closer together, to support how your workforce wishes to work. The IP Phone 8845, 8851, 8861, and 8865 models support this feature. It enables importing of both your contacts and call history from your mobile device to these desk phones. In addition, users have the ability to move the audio path of active voice and video calls to these desk phones to enjoy the superior acoustical properties they can deliver.

Deployment Details

A Unified Communications solution based on the BE6000 can be installed using one of the following methods:

- Standard Deployment - The manual process for installing and configuring applications. This design guide focuses on the standard deployment procedure.

This guide explains how to use Cisco Prime Collaboration Provisioning (PCP) to configure and deploy basic telephony and voice messaging services. This turnkey solution is easy and quick. It also provides a solid foundation for further configuration and deployment of advanced unified communications features, without the need to redesign or reengineer when a new element or service is added.

Easy Access Configuration Sheet

The following table lists the information you will require to complete a standard deployment. Enter your details in the right column. The center column lists the values used as examples throughout this CVD. Use this information to help map your requirements to the procedures detailed in this document.

Cisco Unified CM Installation Requirements		
Item	CVD Configuration	Site-specific Configuration
NTP server IP address	10.64.58.50	
Domain Name System server IP	10.106.170.130	
Domain Name	mmcvd.ciscolabs.com	
Hostname	CUCM-Pub	
IP address	10.106.170.135	
Network mask	255.255.255.128	
Default gateway	10.106.170.129	
Administrator ID	Admin	
Password for admin	[Password]	
Security password	[Password]	
Application username	CUCMAdmin	
Password for CUCMAdmin	[Password]	
Organization	Cisco Systems, Inc	
Unit	Collaboration	
Location	Bangalore	
State	Karnataka	
Country	India	
Lightweight Directory Access protocol (LDAP) information for AD integration: Manager Distinguished name	CN=Administrator,cn=Users,dc=mmcvd,dc=ciscolabs,dc=com	
User search Base	CN=Users,dc=mmcvd,dc=ciscolabs,dc=com	
LDAP server IP address	10.106.170.130	
License files	Obtained from Cisco Licensing team	

Tech Tip

As your solution grows, you may need to acquire a security certificate from a public certification authority. Choose a domain name in this step with a valid Internet domain suffix (.com, .edu, etc) to ensure that your system is ready for this requirement.

Tech Tip

The password must start with an alphabetic character and have at least six characters. It can contain alphanumeric characters, hyphens, or underscores.

Preparing the Network for IP Phones

PROCESS

1. Enable DHCP option 150

The campus design is voice-ready because it includes the QoS settings, VLANs, and IP subnets needed for voice endpoints. It also includes the Dynamic Host Configuration Protocol (DHCP) scopes for the voice VLANs. However, the DHCP option that automatically directs phones to Unified CM is covered in this module.

Procedure 1 Enable DHCP option 150

DHCP is used by phones to obtain an IP address, subnet mask, default gateway, domain name, DNS addresses, and TFTP server(Unified CM) information. When you are configuring DHCP for use in a Cisco Unified CM deployment, this design recommends a local server or Cisco IOS device to provide DHCP service at each site. This type of deployment ensures that DHCP services are available to remote-site telephony devices during WAN failures.

DHCP option 150 provides the IP addresses of the TFTP servers, which enables the phones to download their configuration files and firmware. This option is added to the voice scopes for wired and wireless networks. Option 150 enables up to two IP addresses to be returned to phones as part of the DHCP scope.

The phone always tries the first address in the list, and it tries the subsequent address only if it cannot establish communications with the first TFTP server. The second address provides a redundancy mechanism that enables phones to obtain TFTP services from another server if their primary TFTP server is unreachable. However, it does not provide dynamic load balancing between the two servers. This design recommends that you configure different ordered address lists of TFTP servers in the DHCP scopes to allow for manual load balancing.

For example:

- In subnet 10.106.170.0/24, option 150: CUCM-Pub (primary), CUCM-Sub (secondary)
- In subnet 10.106.171.0/24, option 150: CUCM-Sub (secondary), CUCM-Pub (primary)

Under normal operations, a phone in subnet 10.106.170.0/24 will request TFTP services from CUCM-Pub, while a phone in subnet 10.106.171.0/24 will use CUCM-Sub. If CUCM-Pub fails, then phones from both subnets will request TFTP services from CUCM-Sub. The method for load sharing between the DHCP scopes is left up to the network administrator, because they will have the best knowledge of how many phones reside in each subnet.

If the remote site has a single WAN router without a distribution layer, the best place for DHCP is on the router. If the remote site has dual WAN routers or a distribution layer, the DHCP service should be located on a standalone server or on a distribution switch.

In all situations, phones need option 150 added to their DHCP scope configurations. If the headquarters site uses the primary TFTP server as the first choice, the remote sites should use the secondary TFTP as the first choice until the phone count is balanced between the two servers.

If you are using a Microsoft DHCP server, complete Option 1 of this procedure. If you are using the Cisco IOS DHCP server feature, complete Option 2.

Option 1: Enable option 150 on Microsoft DHCP server

Use the following commands to enable option 150 on a Microsoft DHCP server.

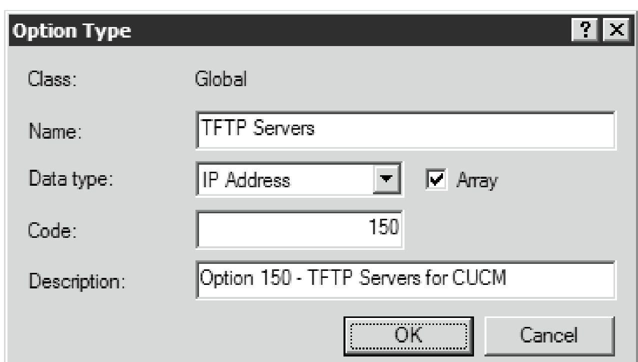
Step 1. From the Microsoft server, open the DHCP Server Administration Tool.

Step 2. On the left side of the page, navigate to [active directory name] > IPv4 (Example: ad.mmcvd.ciscolabs.com > IPv4).

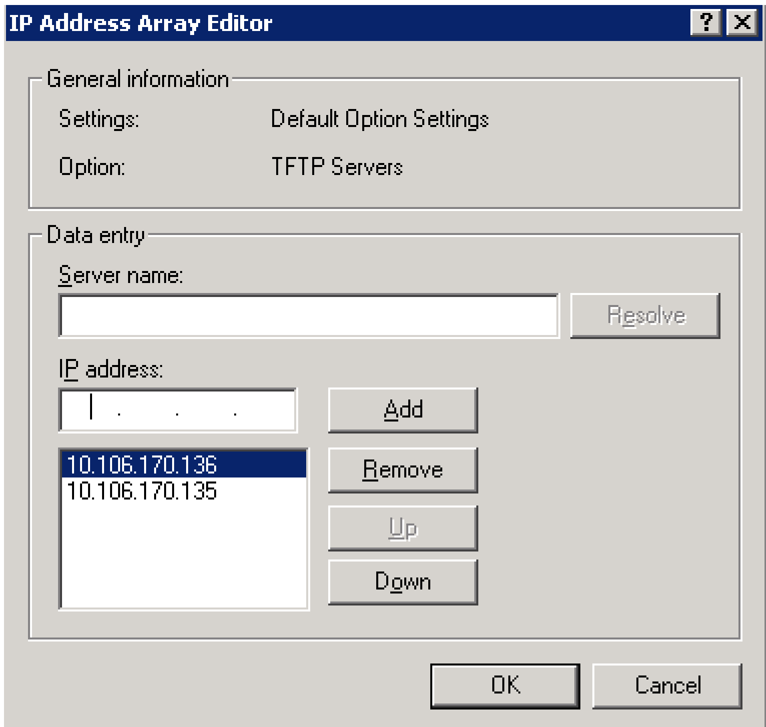
Step 3. Right-click IPv4, and then choose Set Predefined Options from the list.

Step 4. Click Add, enter the following information, and then click OK:

- Name—**TFTP Servers**
- Data Type—**IP Address**
- Array—Select the check box.
- Code—**150**
- Description—**Option 150 - TFTP Servers for CUCM**



Step 5. Click Edit Array, add up to two IP addresses for your TFTP servers, and then click OK.



Step 6. On the Predefined Options and Value page, verify the information and then click OK.

Option 2: Enable option 150 using Cisco IOS DHCP server feature

Use the following commands to enable option 150 in the appropriate DHCP pools in Cisco IOS devices.

Step 1. Log in to the device with a username that has the ability to make configuration changes.

Step 2. In the global configuration section, edit the DHCP pools supporting IP phones to include option 150 so the phones can find the TFTP servers at 10.106.170.136 (secondary) and 10.106.170.135 (primary).

```
ip dhcp pool wired-voice
  network 10.106.170.0 255.255.255.0
  default-router 10.106.170.1
  dns-server 10.106.170.130
  option 150 ip 10.106.170.136 10.106.170.135
  domain-name mmcvd.ciscolabs.com

ip dhcp pool wired-voice2
  network 10.106.171.0 255.255.255.0
```

```
default-router 10.106.171.1
dns-server 10.106.170.130
option 150 ip 10.106.170.136 10.106.170.135
domain-name mmcvd.ciscolabs.com
```

Network Preparation Summary

To ensure that your phones are registered at the correct time, you need to deploy DHCP option 150 and select your IP phone models before you perform the deployment procedures found in the next process.

During the software installation, the server performs a reverse DNS lookup on the name and IP address entered. The installation halts if the lookup does not succeed, so please verify that the server information is properly entered into DNS and that the associated pointer records are created beforehand.

Preparing the Server for Cisco Unified CM

PROCESS

1. Configure server connectivity to the LAN
2. Prepare the server for Unified CM

The BE6000 server includes a software summary in the data store that lists the applications included - so you would know the software available and what might be newer on the website.

To install Cisco Unified CM, make sure you have completed the following steps before you start:

- Download the Open Virtual Archive (OVA) virtual machine template from the Cisco website at: https://software.cisco.com/download/home/286313357/type/283088407/release/12.0%25281%2529
- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM: https://software.cisco.com/download/home/286313357/type/286319236/release/12.0%25281%2529SU2

Procedure 1 — Configure platform connectivity to the LAN

The Cisco BE6000 server can be connected to a Cisco switch in the data center or a Cisco Catalyst switch in the server room. Please choose the option that is appropriate for your environment.

Option 1: Connect the server to a Cisco switch

Step 1. Log in to the Cisco switch with a username that has the ability to make configuration changes.

Step 2. If there is a previous configuration on the switch port where the Cisco Unified BE6000 server is connected, remove the individual commands by issuing a no in front of each one. This brings the port back to its default state.

Step 3. Configure the port as an access port.

```
interface Ethernet1/1/4
 description BE6000
 switchport access vlan 20
```

Option 2: Connect the BE6000 server to a Cisco Catalyst switch

Step 1. Log in to the Cisco Catalyst switch with a username that has the ability to make configuration changes.

Step 2. Clear the interface's configuration on the switch port where the Cisco Unified CM server is connected.

```
default interface GigabitEthernet1/0/6
```

Step 3. Configure the port as an access port.

```
interface GigabitEthernet1/0/6
 description Unified CM
 switchport access vlan 20
```

Procedure 2	Prepare the server for Unified CM

This BE6000 server comes preloaded with a bootable image of Cisco Unified CM. Power on the server and start configuring.

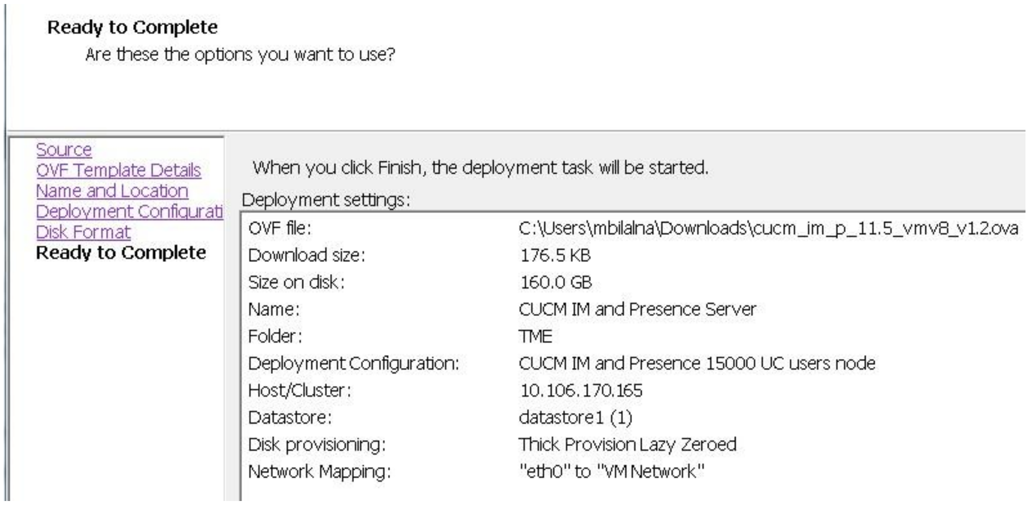
If you are deploying a secondary server, then follow the steps below to deploy an OVA file in order to define the virtual machine requirements.

Step 1. Open VMware vSphere Client, click the server hardware you want to use for this install, and then navigate to File > Deploy OVF Template.

Step 2. In the Deploy OVF Template wizard, enter the following information:

- On the Source page, click Browse, select the Cisco Unified CM OVA file downloaded from Cisco or from the datastore of the BE6000 server, click Open, and then click Next.
- On the OVF Template Details page, verify the version information, and then click Next:
- On the Name and Location page, in the Name box, enter the virtual machine name CUCM-Pub. In the Inventory Location tree, select the location to deploy the server, and then click Next.
- On the Deployment Configuration page, in the Configuration list, choose the following node, and then click Next.
    - 1000-user node (BE6000)—for a cluster of 1000 or fewer users.
- On the Disk Format page, choose Thick Provision Eager Zeroed, and then click Next.

On the Ready to Complete page, verify the settings, and then click Finish.



Step 3. In the message window, click Close.

Step 4. After the virtual machine is created, click on the server name, (Example: CUCM-Pub), navigate to the Getting Started tab, and then click **Edit virtual machine settings**.

Step 5. On the Hardware tab, select CD/DVD Drive 1, and then select Connect at power on.

Step 6. Select Datastore ISO File, click Browse, navigate to the location of the Cisco Unified CM bootable installation file (or browse the datastore to find the Unified CM installation file), select the correct ISO image, and then click OK.

Step 7. On the Getting Started tab, click Power on virtual machine.

Step 8. Click the Console tab, and then watch the server boot. After the ISO loads, the virtual machine is prepared for installation.

Installing Cisco Unified CM

PROCESS

Procedure 1 Install the first Cisco Unified CM platform

Refer to the installation guide for installing the Cisco Unified CM.

Procedure 2 Install licenses and start services

After the first Cisco Unified CM platform is installed, there are several configuration steps that have to be completed in order to prepare the publisher for the remaining servers.

Step 1. In a web browser, access the IP address or hostname of the publisher, and then in the center of the page, under Installed Applications, click Cisco Prime License Manager.

Step 2. On the login page, enter the following application username and password and then click Login:

- User Name—**CUCMAdmin** (case-sensitive)
- Password—**[password]**

Step 3. Navigate to Inventory > Product Instances, and then click Add.

> *i* Tech Tip
>
> The username and password for adding the product instances is the case-sensitive platform administrator ID that was created when installing the server software.

Step 4. Enter the following information for Cisco Unified CM, and then click Test Connection:

- Name—**CUCM-Pub**
- Description—**CUCM Publisher**
- Product Type—**Unified CM**
- Hostname/IP Address—**10.106.170.135 (publisher)**
- Username—**Admin** (case-sensitive platform administrator ID)
- Password—**[password]**

Step 5. In the message window, click OK.

Step 6. If the connection is successful, click OK.

If the connection is not successful, repeat Step 4 through Step 6 with the correct information.

Step 7. Click Synchronize Now.

Step 8. Navigate to Licenses > Fulfillment, and then select Other Fulfillment Options > Fulfill Licenses from File.

i	Tech Tip

Extract the .bin file from the .zip before trying to install the license in the next step. The installation process returns an error if you try to install the .zip file.

Step 9. On the Install License File page, click Browse, locate the directory that contains the license files you obtained prior to installation, select the .bin file, click Open, and then click Install. A message confirms that the license is successfully installed.

Step 10. Repeat Step 8 through Step 9 for each additional license file for your installation. After all files are installed, click Close. Verify that the licenses are successfully installed.

Step 11. Navigate to Monitoring > License Usage, and then confirm the status is In Compliance. If there is a problem, please notify your Cisco representative in order to obtain new license files.

Step 12. In a web browser, access the IP address or hostname of the publisher, and in the center of the page, under Installed Applications, click Cisco Unified Communications Manager.

Step 13. Enter the Username and Password from the Application User Configuration page in Step 2 of the previous procedure, and then click Login.

Step 14. In the Navigation list at the top of the page, choose Cisco Unified Serviceability, and then click Go.

Step 15. Navigate to Tools > Service Activation, in the Server list, choose CUCM-Pub, and then click Go.

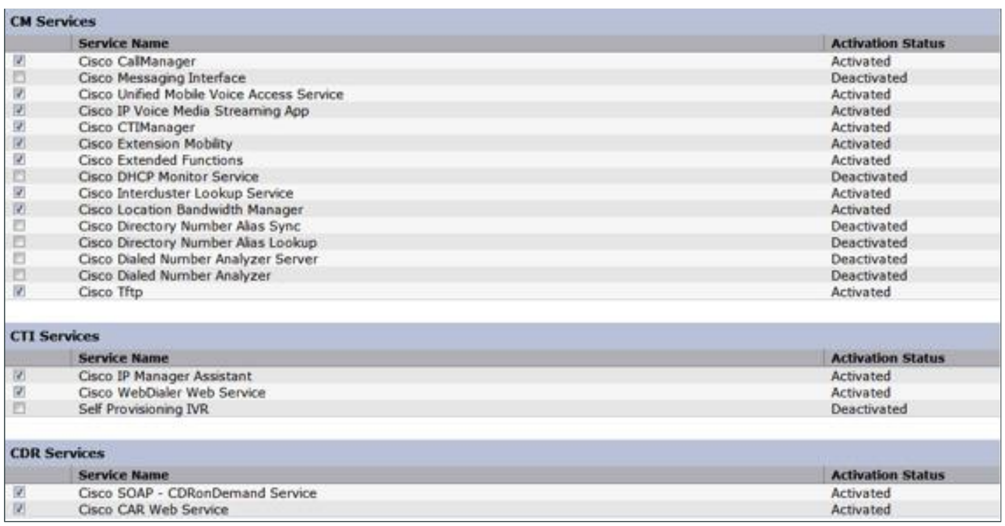
Step 16. Select Check All Services, clear the ones that are not needed for this node, and then click Save.

i	Tech Tip

You may safely disable the following services if you don’t plan to use them:

- Cisco Messaging Interface
- Cisco DHCP Monitor Service
- Cisco TAPS Service
- Cisco Directory Number Alias Sync
- Cisco Directory Number Alias Sync
- Cisco Dialed Number Analyzer Server
- Cisco Dialed Number Analyzer
- Self Provisioning IVR

Step 17. In the message window, click OK.



CM Services

Service Name	Activation Status
Cisco CallManager	Activated
Cisco Messaging Interface	Deactivated
Cisco Unified Mobile Voice Access Service	Activated
Cisco IP Voice Media Streaming App	Activated
Cisco CTIManager	Activated
Cisco Extension Mobility	Activated
Cisco Extended Functions	Activated
Cisco DHCP Monitor Service	Deactivated
Cisco Intercluster Lookup Service	Activated
Cisco Location Bandwidth Manager	Activated
Cisco Directory Number Alias Sync	Deactivated
Cisco Directory Number Alias Lookup	Deactivated
Cisco Dialed Number Analyzer Server	Deactivated
Cisco Dialed Number Analyzer	Deactivated
Cisco Tftp	Activated

CTI Services

Service Name	Activation Status
Cisco IP Manager Assistant	Activated
Cisco WebDialer Web Service	Activated
Self Provisioning IVR	Deactivated

CDR Services

Service Name	Activation Status
Cisco SOAP - CDRonDemand Service	Activated
Cisco CAR Web Service	Activated

Figure 10. Recommended Publisher Services when using a Non-dedicated TFTP Server

Activating services may take a few minutes to complete, so please wait for the page to refresh before you continue.

Procedure 3 Configure Additional Servers

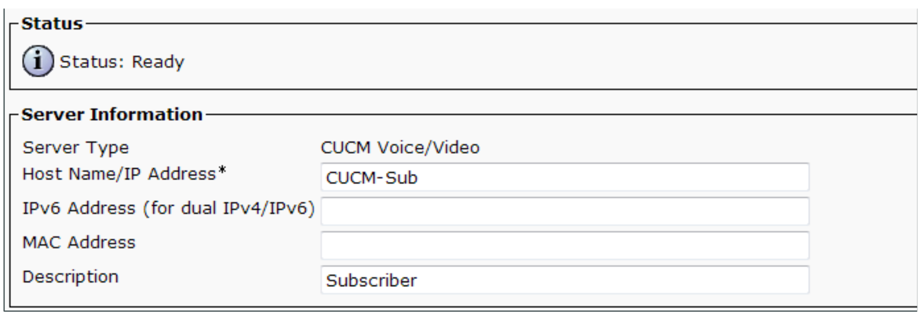
After installing the licenses and starting the services, the subscribers, TFTP and voicemail servers must be added to the publisher. When new subscribers and TFTP servers are added to a publisher, the initial use of host names makes it easier to identify the servers for troubleshooting purposes. The host names will be changed to IP addresses later in this guide.

Step 1. In the Navigation list at the top of the page, choose Cisco Unified CM Administration and then click Go.

Step 2. Navigate to System > Server, and then click Add New.

Step 3. Select the server type as CUCM Voice/Video.

Step 4. Enter the host name of the additional Cisco Unified CM server, a description, and then click Save.



The next steps add Cisco Unity Connection as an application server to the cluster.

Step 5. Navigate to System > Application Server, and then click Add New.

Step 6. On the first Application Server Configuration page, in Application Server Type list, choose Cisco Unity Connection, and then click Next.

Step 7. On the second Application Server Configuration page, in the Name box, enter **CUC**, and then in the IP Address box, enter **10.106.170.137**.

Step 8. In the Available Application Users list, select the account you created during the installation of Cisco Unified CM (Example: CUCMAdmin), move the account to the Selected Application Users list by clicking the v character, and then click Save.

Step 9. When the subscriber and Cisco Unity Connection servers are added to the publisher's database, repeat the procedures in "Preparing the Platform for Cisco Unified CM" for each additional Unified CM server, and then return to Procedure 4, "Install the redundant server."

Procedure 4	Install the Redundant Server

Install the redundant server(subscriber) with the same steps as listed in the Installation guide.

Procedure 5	Start Services

After the software installation completes, the services must be started from the subscriber.

Step 1. In a web browser, access the Cisco Unified CM administration interface on the publisher, and then in the center of the page, under Installed Applications, click Cisco Unified Communications Manager.

Step 2. Enter the application Username and Password, and then click Login.

Step 3. In the Navigation list on the top right side of the page, choose Cisco Unified Serviceability, and then click Go.

Step 4. Navigate to Tools > Service Activation.

Step 5. In the Server list, choose the next additional server, and then click Go.

Step 6. Select Check All Services, clear the ones that are not needed for this node, and then click Save.

Step 7. In the message window, click OK.

Figure 11. Recommended Subscriber Services when using Non-dedicated TFTP Servers

CM Services

Service Name	Activation Status
Cisco CallManager	Activated
Cisco IP Voice Media Streaming App	Activated
Cisco CTIManager	Activated
Cisco Extension Mobility	Activated
Cisco Extended Functions	Activated
Cisco DHCP Monitor Service	Deactivated
Cisco Location Bandwidth Manager	Activated
Cisco Directory Number Alias Lookup	Deactivated
Cisco Dialed Number Analyzer Server	Deactivated
Cisco Dialed Number Analyzer	Deactivated
Cisco Tftp	Activated

CTI Services

Service Name	Activation Status
Cisco IP Manager Assistant	Activated
Cisco WebDialer Web Service	Activated

Database and Admin Services

Service Name	Activation Status
Cisco AXL Web Service	Activated
Cisco UXL Web Service	Activated

Performance and Monitoring Services

Service Name	Activation Status
Cisco Serviceability Reporter	Activated
Cisco CallManager SNMP Service	Activated

Security Services

Service Name	Activation Status
Cisco CTL Provider	Activated

Activating services may take a few minutes to complete, so please wait for the page to refresh before continuing.

Procedure 6 Adding the Secondary Node in the Cisco Unified Communications Manager Group

Step 1. In a web browser, access the Cisco Unified CM administration interface on the publisher, and then in the center of the page, under Installed Applications, click **Cisco Unified Communications Manager.**

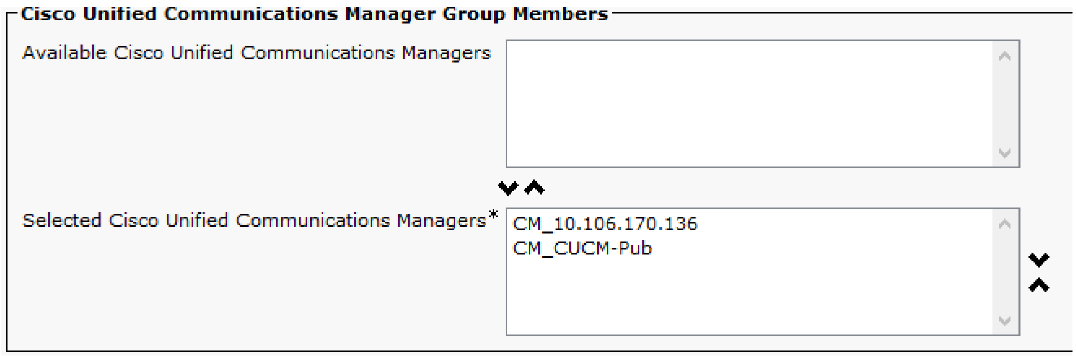
Step 2. Enter the application Username and Password, and then click Login.

Step 3. In the Navigation list on the top right side of the page, choose Cisco Unified CM, and then click Go.

Step 4. Navigate to **System>Cisco Unified CM group.**

Step 5. Select the secondary Cisco Unified Communications Manager from the Available group and click the down arrow.

Step 6. Click save.


Cisco Unified Communications Manager Group Members
Available Cisco Unified Communications Managers
Selected Cisco Unified Communications Managers*
CM_10.106.170.136
CM_CUCM-Pub

Preparing the Platform for Cisco Unity Connection

Easy Access Configuration Sheet

The following information is needed for the installation:

Cisco Unity Connection Installation Requirements		
Item	CVD Configuration	Site-specific Configuration
NTP server IP address	10.64.58.50	
Domain Name System server IP	10.106.170.130	
Domain Name	mmcvd.ciscolabs.com	
Hostname	CUC	
IP address	10.106.170.137	
Network Mask	255.255.255.128	
Default gateway	10.106.170.129	
Administrator ID	Admin	
Admin password	[Password]	
Security password	[Password]	
Application username	CUCAdmin	
Application password	[password]	
Organization	Cisco Systems, Inc	
Unit	Collaboration	
Location	Bangalore	
State	Karnataka	
Country	India	
Lightweight Directory Access protocol (LDAP) information for AD integration:	CN=Administrator,cn=Users,dc=mmcvd,dc=ciscolabs,dc=com	
Manager Distinguished name User search Base	CN=Users,dc=mmcvd,dc=ciscolabs,dc=com	
LDAP server IP address	10.106.170.130	

i	Tech Tip
The password must start with an alphabetic character and have at least six characters, and it can contain alphanumeric characters, hyphens, or underscores. The default pin generated by the PCP for Voicemail is 054321.	

Cisco Unity Connection is used as the voicemail platform for the unified communications foundation. It is configured as a simple voicemail-only system that uses a single server.

The BE6000 server includes a software summary in the data store that lists the applications included - so you would know the software available and what might be newer on the website

For a quick and easy installation experience, it is essential to know up front what information you will need. To install Cisco Unity Connection, make sure you have completed the following steps before you start:

Download the Open Virtual Archive (OVA) file from the Cisco website at: https://software.cisco.com/download/home/283062758/type/282074348/release/OVA-12.0

- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM:

  https://software.cisco.com/download/home/286313379/type/286319533/release/12.0%25281%2529SU2

Installing Cisco Unity Connection

PROCESS

1. Install Cisco Unity Connection platform
2. Install licenses and start services

Procedure 1 Install Cisco Unity Connection server

For installation of Cisco Unity Connetction, refer to the installation guide.

Procedure 2 Install Licenses and Start Services

After the Unity Connection platform is installed, there are several configuration steps that have to be completed in order to add the licenses and start the services.

Step 1. In a web browser, access the Cisco Unified CM publisher, and in the center of the page, under Installed Applications, click Cisco Prime License Manager.

Step 2. On the login page, enter the following case-sensitive Cisco Unified CM application username and password, and then click Login:

- User Name—**CUCMAdmin** (case-sensitive)
- Password—**[password]**

Step 3. Navigate to Inventory > Product Instances, and then click Add.

i	Tech Tip

The username and password for adding the Product Instances is the case-sensitive platform administrator ID that was entered when installing the server software.

Step 4. Enter the following information for Cisco Unity Connection, and then click Test Connection:

- Name—**CUC**
- Description—**Unity Connection**
- Product Type—**Unity Connection**

- Hostname/IP Address—**10.106.170.137**
- Username—**Admin**
- Password—**[password]**

Step 5. In the message window, click OK.

Step 6. If the connection is successful, click OK.

If the connection is not successful, repeat Step 4 through Step 6 with the correct information.

Step 7. Click Synchronize Now.

Step 8. Navigate to Licenses> Fulfillment and then select Other Fulfillment Options > Fulfill Licenses from File.

Step 9. On the Install License File page, click Browse, locate the directory that contains the license files you obtained prior to installation, select the .bin file, click Open, and then click Install.

Step 10. Repeat Step 9 for each additional license file for your installation. After all files are installed, click Close.

Next, you verify that the licenses are installed successfully.

Step 11. Navigate to Licenses > Usage, and then confirm the status is In Compliance.

If there is a problem, please notify your Cisco representative in order to obtain new license files.

Step 12. In a web browser, access the Cisco Unity Connection server, and then in the center of the page, under Installed Applications, click Cisco Unity Connection.

Step 13. Enter the Username and Password you entered on the Application User Configuration page in Step 18 of the previous procedure, and then click Login.

Step 14. In the Navigation list, choose Cisco Unified Serviceability, and then click Go.

Step 15. Navigate to Tools > Service Activation, select Check All Services, and then click Save. In the message window, click OK.

Activating services may take a few minutes to complete, so wait for the page to refresh before you continue.

Preparing the server for Cisco Unified CM IM and Presence

Easy Access Configuration Sheet

The following information is needed for the installation

Cisco Unified CM IM and Presence Installation requirements		
Item	CVD Configuration	Site-specific Configuration
NTP server IP address	10.64.58.50	
Domain Name System server IP	10.106.170.130	
Domain Name	mmcvd.ciscolabs.com	
Hostname, IP address	IMP	
IP address	10.106.170.146	
Network Mask	255.255.255.128	
Default Gateway	10.106.170.129	
Administrator ID	Admin	
Password	[Password]	
Organization	Cisco Systems, Inc	
Unit	Collaboration	
Location	Bangalore	
State	Karnataka	
Country	India	
Connectivity to First node (UCM Publisher): Hostname	CUCM-Pub	
UCM IP address	10.106.170.135	
UCM security password	[Password]	

> **i** Tech Tip
>
> The password must start with an alphabetic character and have at least six characters. It can contain alphanumeric characters, hyphens, or underscores.

The BE6000 server includes a software summary in the data store that lists the applications included - so you would know which software is available, and what might be latest on the website.

For a quick and easy installation experience, it is essential to know upfront what information you will need. For Cisco Unified CM Instant Messaging and Presence, make sure you have completed the following steps before you start:

- Download the Open Virtualization Archive (OVA) file from the Cisco website at: https://software.cisco.com/download/home/286318790/type/282074312/release/UTILS
- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM IM and Presence: https://software.cisco.com/download/home/286318790/type/282074312/release/UTILS

Installing Cisco Unified CM IM and Presence

PROCESS

1. Install Cisco Unified CM IM and Presence
2. Start services

Procedure 1 Install Cisco Unified CM IM and Presence

For installation of Cisco Unified CM IM & Presence, refer to the Installation Guide.

Procedure 2 Start Services

After the software is installed, use the web interface to complete the rest of the procedures.

Step 1. In a web browser, enter the IP address or hostname of the Cisco Unified CM IM and Presence server, and then in the center of the page under Administrative Applications, click Cisco Unified Communications Manager IM and Presence.

> *i* Tech Tip
>
> If you receive a message about the website's security certificate, ignore it and continue on the page.

Step 2. In the Navigation list, click Cisco Unified CM IM and Presence administration, and then click Go.

Step 3. Enter the username and password of the Unified CM admin.

Step 4. Navigate to Tools > Service Activation, enter the following information, and then click Save:

- Cisco SIP Proxy—**Select**
- Cisco Presence Engine—**Select**
- Cisco Sync Agent—**Select**
- Cisco XCP Connection Manager—**Select**
- Cisco XCP Directory Service—**Select**
- Cisco XCP Authentication Service—**Select**

IM and Presence Services

	Service Name	Activation Status
☑	Cisco SIP Proxy	Activated
☑	Cisco Presence Engine	Activated
☑	Cisco Sync Agent	Activated
☐	Cisco XCP Text Conference Manager	Deactivated
☐	Cisco XCP Web Connection Manager	Deactivated
☑	Cisco XCP Connection Manager	Activated
☐	Cisco XCP SIP Federation Connection Manager	Deactivated
☐	Cisco XCP XMPP Federation Connection Manager	Deactivated
☐	Cisco XCP Message Archiver	Deactivated
☑	Cisco XCP Directory Service	Activated
☑	Cisco XCP Authentication Service	Activated

Database and Admin Services

	Service Name	Activation Status
☐	Cisco AXL Web Service	Deactivated
☐	Platform SOAP Services	Deactivated
☐	Cisco Bulk Provisioning Service	Deactivated

Performance and Monitoring Services

	Service Name	Activation Status

Step 5. In the message window, click OK.

Preparing the server for Cisco Prime Collaboration Provisioning

Easy Access Configuration Sheet

The following information is needed for the installation:

Cisco Prime Collaboration Installation Requirements		
Item	CVD Configuration	Site-specific Configuration
NTP server IP address	10.64.58.50	
Domain Name System server IP	10.106.170.130	
Domain Name	mmcvd.ciscolabs.com	
Hostname	CPC	
IP address	10.106.170.139	
Network Mask	255.255.255.128	
Default Gateway	10.106.170.129	
Globaladmin password	[Password]	
Security password	[Password]	
Root password	[password]	
Lightweight Directory Access protocol (LDAP) information for AD integration	CN=Administrator,cn=Users,dc=mmcvd,dc=ciscolabs,dc=com	
Manager Distinguished name User search Base	CN=Users,dc=mmcvd,dc=ciscolabs,dc=com	
LDAP server IP address	10.106.170.130	

i	Tech Tip
	The password must start with an alphabetic character and have at least six characters, and it can contain alphanumeric characters, hyphens, or underscores.

The BE6000 server includes a software summary in the data store that lists the applications included - so you would know the software available and what might be newer on the website.

For a quick and easy installation experience, it is essential to know upfront what information you will need. For Cisco Prime Collaboration Provisioning, make sure you have completed the following steps before you start:

Download the Open Virtualization Archive (OVA) file from Cisco website at:
https://software.cisco.com/download/home/286321363/type/286289070/release/12.5

Installing Cisco Prime Collaboration Provisioning

PROCESS

1. Install Cisco Prime Collaboration Provisioning
2. Configure Cisco Unified Communication processors using Cisco Prime Collabration Provisioning

Procedure 1	Install Cisco Prime Collaboration Provisioning

For installation of Cisco Prime Collaboration Provisioning, refer to the Installation Guide.

Configuring Cisco Unified CM using Cisco Prime Collaboration Provisioning

Procedure 1	Configure Cisco Unified Communication processors using Cisco Prime Collaboration Provisioning

After the software is installed, use the web interface to complete the rest of the procedures.

Step 1. In a web browser, enter the IP address or hostname of the Cisco Prime Collaboration Provisioning server.

Step 2. Enter the globaladmin username and password of the Cisco Prime Collaboration Provisioning server.

When you log into Cisco Prime Collaboration Provisioning for the first time, the Getting Started Wizard (GSW) pop up window appears. On subsequent logins, you must choose **Infrastructure Setup > Getting Started Wizard**.

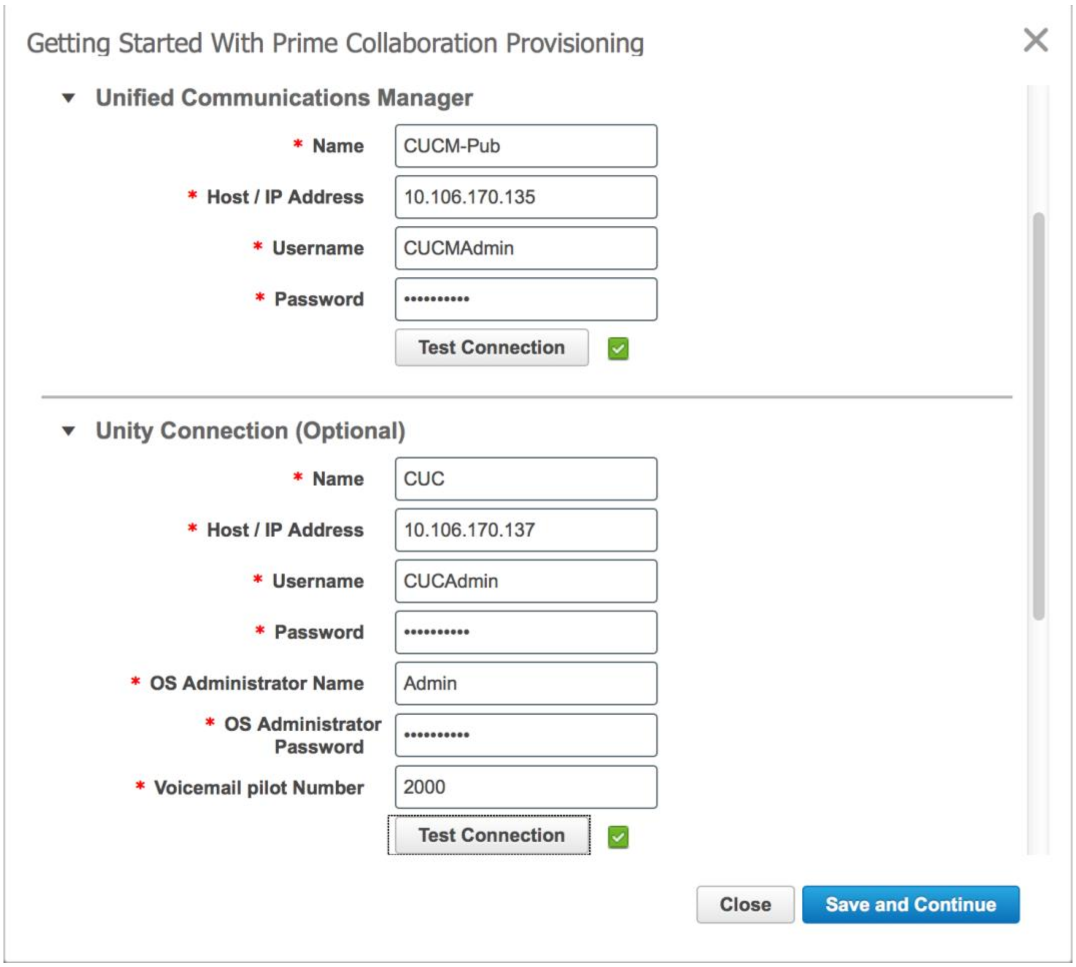
If you have a configuration file that contains configuration details, you can upload it manually using the **Use Existing Configuration** step, or just click **Begin**, to start the configuration.

Step 3. Set up your devices. In the following examples, all the unified communication server credentials are populated with an example value. Replace all the values with the specific details of your infrastructure devices from the Before you Start table.

i	Tech Tip

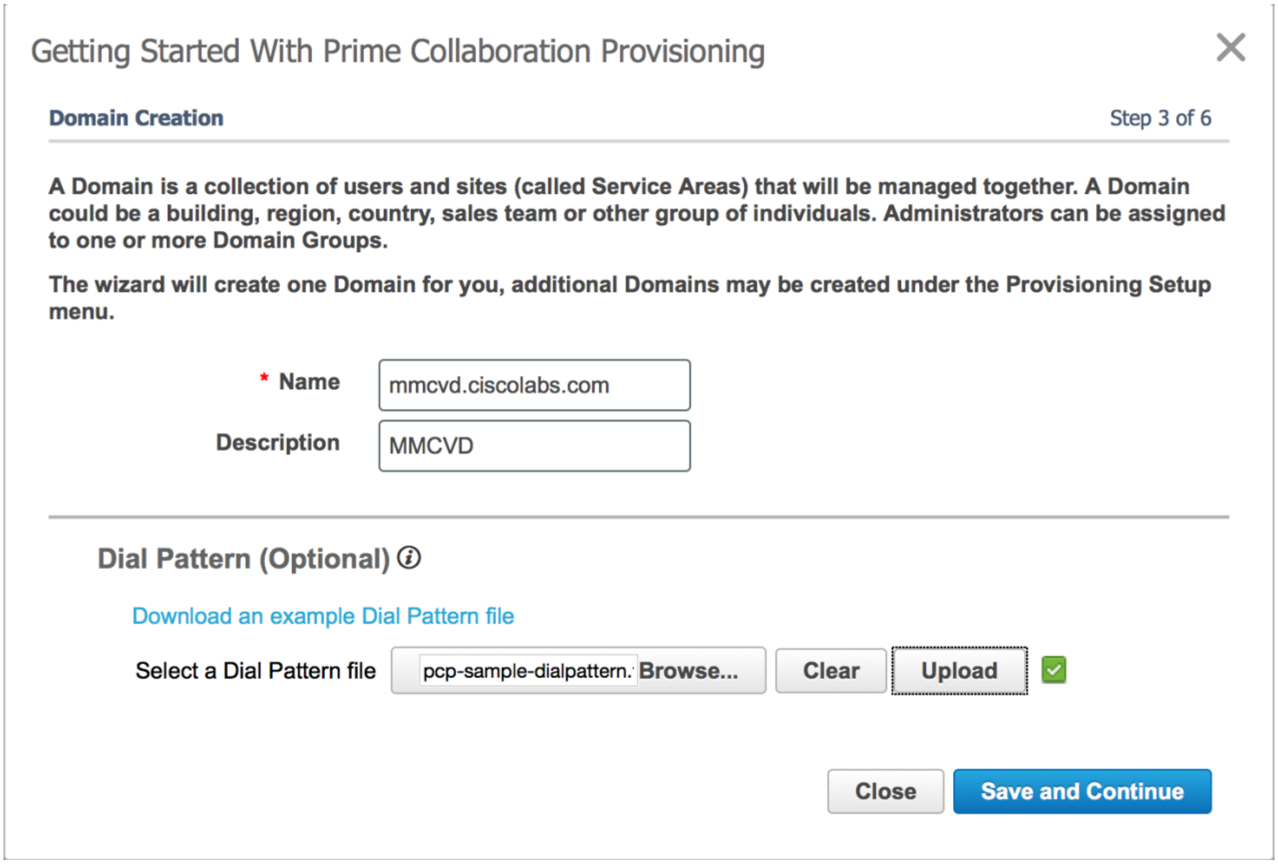
Make sure you enter the right values, because you can’t go back and change the values once you proceed.

- Unified Communications Manager
  Name > CUCM-Pub
  Host / IP Address > 10.106.170.135
  Username > CUCMAdmin
  Password > **********
    Click Test connection
    It should have a green check mark if not re verify the credential
- Unity Connection (optional)
  Name > CUC
  Host / IP Address > 10.106.170.137
  Username > CUCAdmin
  Password > **********
    OS Administrator Name : Admin
    OS Administrator Password : *********
    Voicemail pilot Number : 2000
    Click Test connection
    It should have a green check mark if not re verify the credential
- Do not check **Enable Unified Messaging** (requires Exchange Server information).
- Unified IM & Presence (Optional)
  Name > IMP1
  Host / IP Address > 10.106.170.146
  Username > CUCMAdmin
  Password > **********
  Click **Test Connection**.
  It should have a green check mark if not re verify the credential
- Click **Save and Continue**.



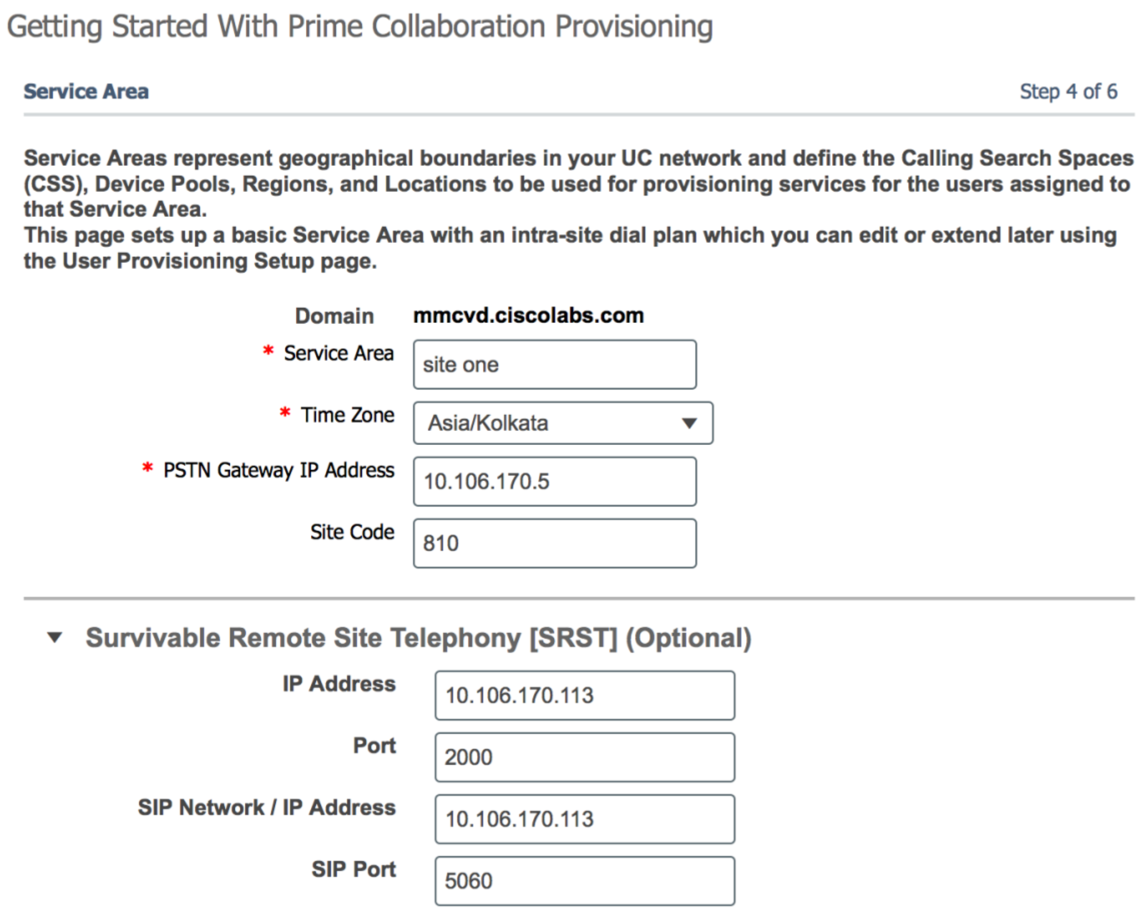
Step 4. Create an administrative Domain as follows:

- Enter a domain name and description.
- Right-click on the **Download an example Dial Pattern** file, and save and upload the dial pattern file. A green check mark is displayed on uploading the dial pattern. Click **Save and Continue**.



Step 5. Create a Service Area. Enter a Service area name and the following details, when prompted.

- Service area > Site one
- Time Zone > Asia/Kolkata
- PSTN Gateway IP Address > 10.106.170.5
- Site Code > 810
- SRST details:
    - IP Address > 10.106.170.113
    - Port > 2000
    - SIP Network / IP Address > 10.106.170.113
    - SIP Port > 5060



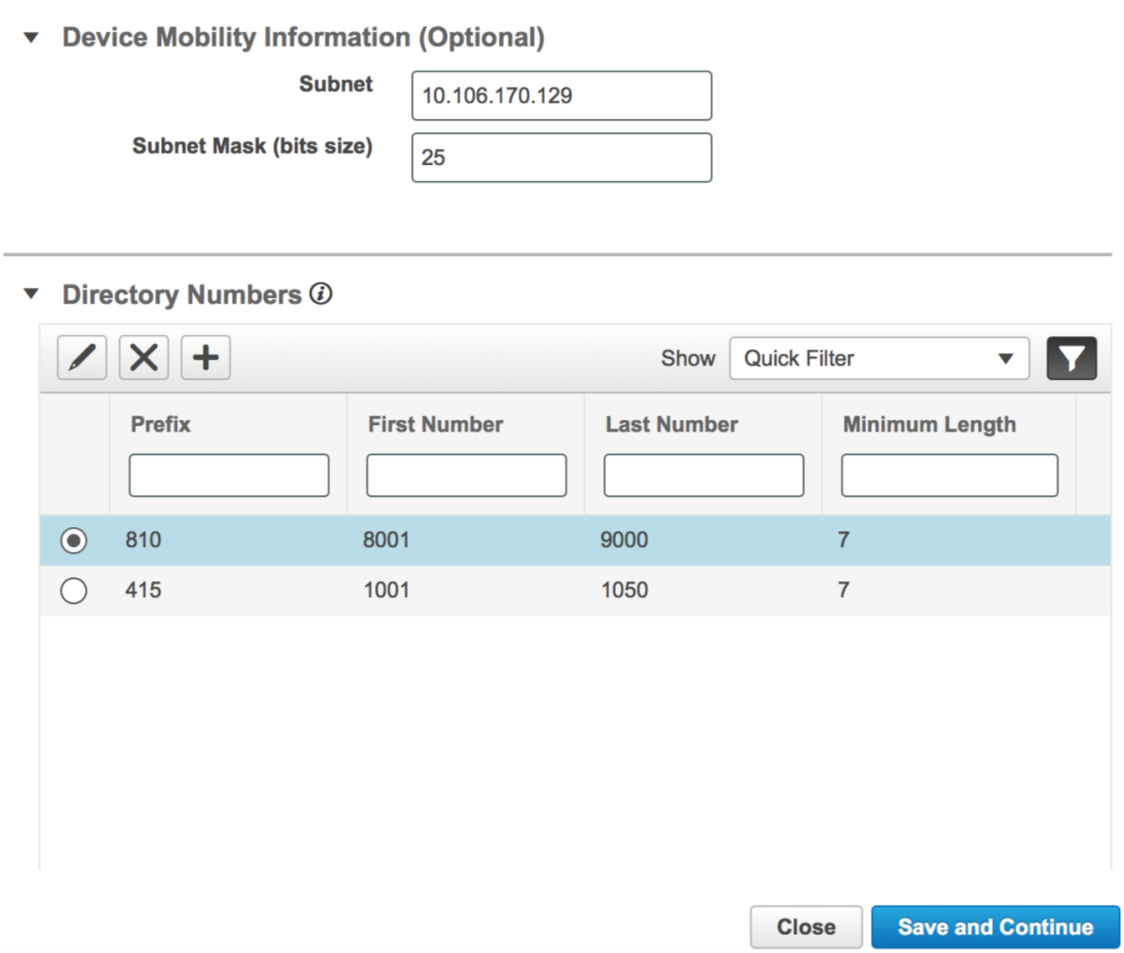
Step 6. Enter the following Device Mobility details:

- Subnet > 10.106.170.129
- Subnet Mask (bits size) > 25

Step 7. Enter the following Directory Numbers details:

- Click **Edit** and change the Prefix, First number, and Last Number accordingly.
- Prefix > 810
- First Number >8001 Last Number > 9000

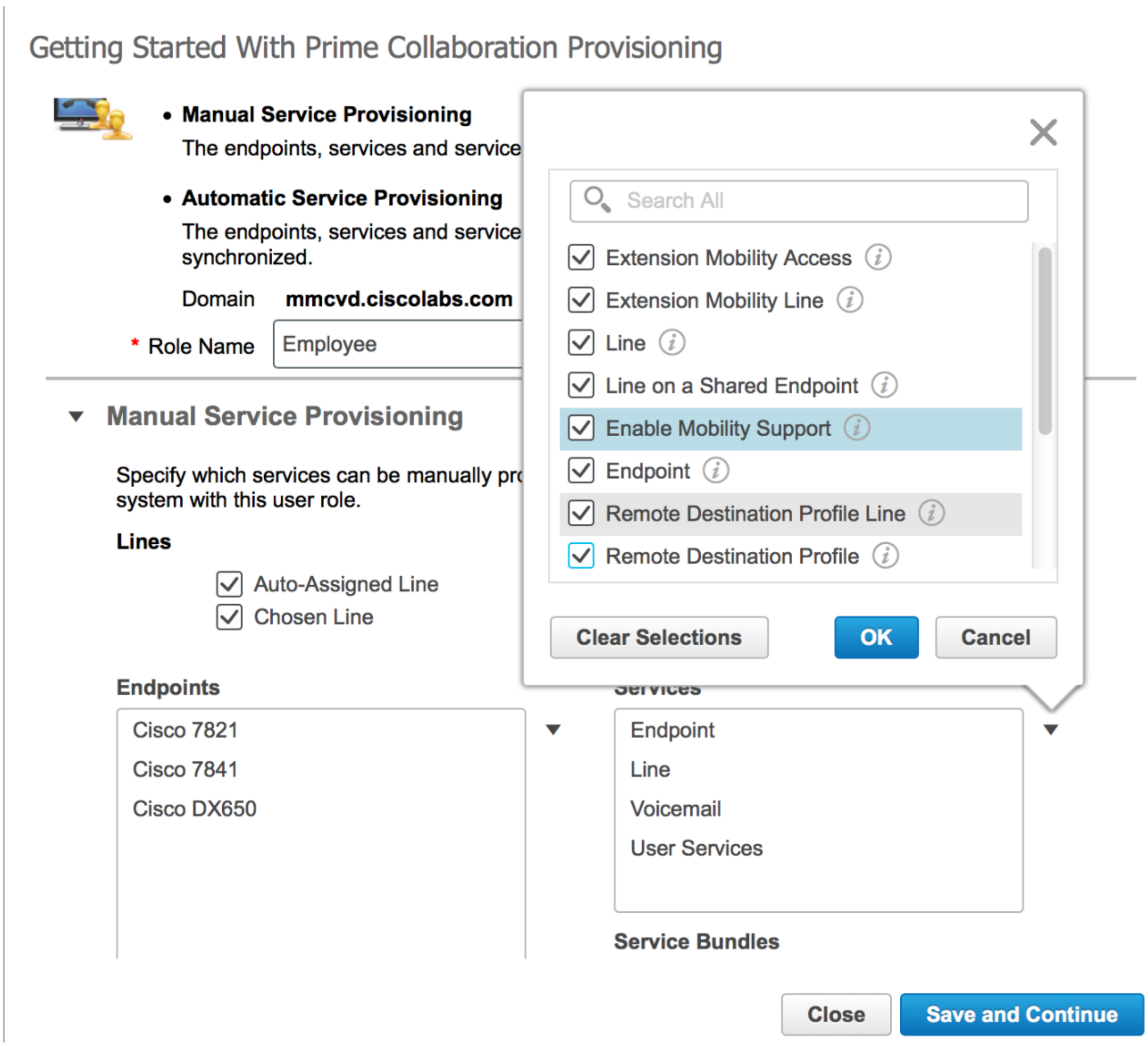
Click **Save and Continue**.



Step 8. Select Role Name as Employee in the User Role (Part 1 - Manual Service Provisioning) field of the GSW.

Step 9. At the Manual Service Provisioning pane, do the following:

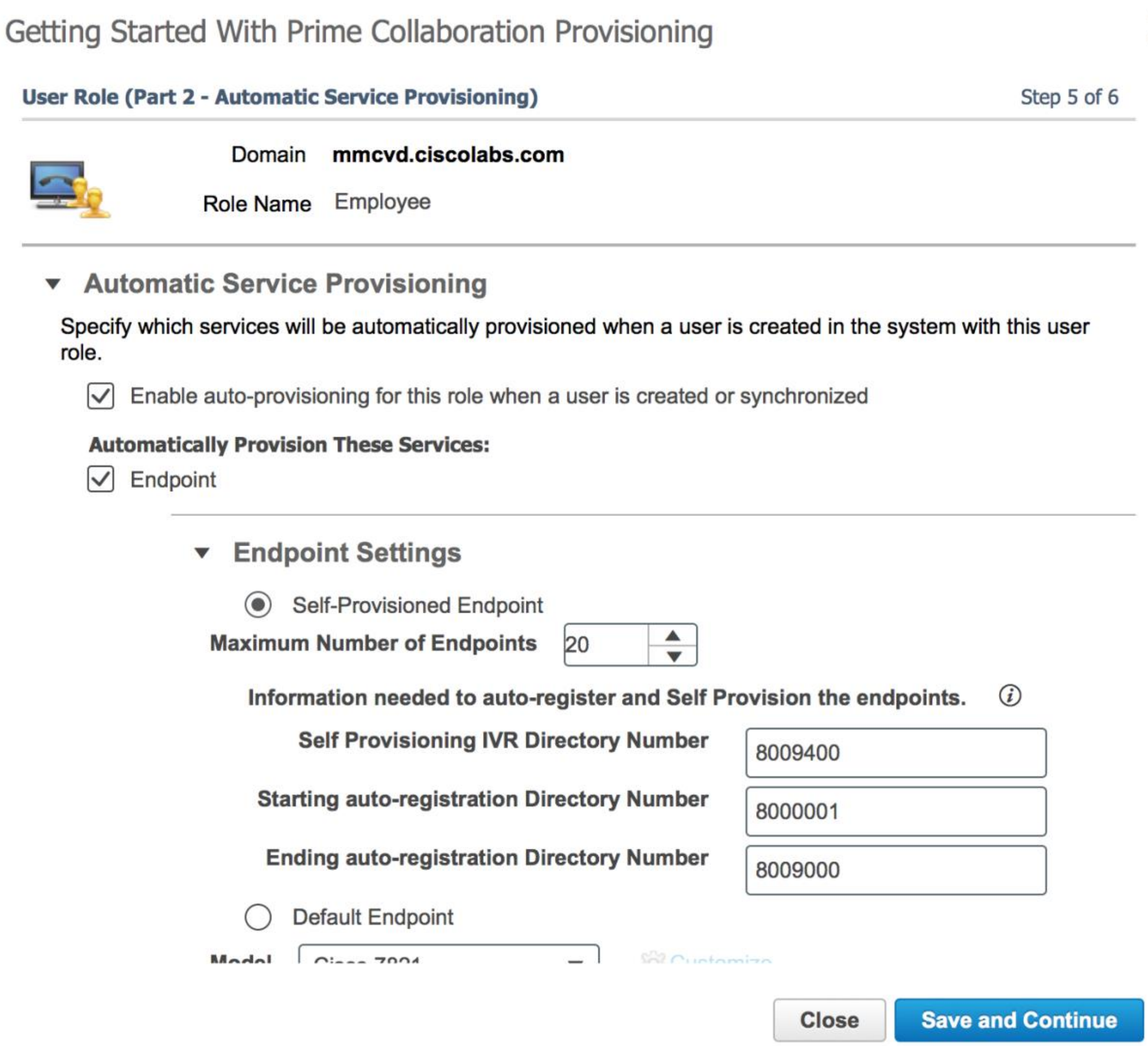
- Check or clear the Line and Chosen Line depending on the kind of line needed.
- Under the **Endpoint** field, click on the corresponding check box and select the chosen endpoint type from the drop-down list..
- Under the **Services** field, click the check box, and make your selection in the drop-down list.
- Under the **Service Bundle** field click on the check box and then selct from the drop-down list.
- Click **Save and Continue**.



Step 10. Set up **Automatic Service Provisioning. Select the Enable auto-provisioning for this role when a user is created or synchronized** check box.

- Under the **Automatically Provision These Services** pane, select the **Endpoint** check box.
- Under the **Endpoint Settings** pane, select the **Self-provisioned Endpoint** option, and set the maximum number of self-provisioned Endpoints a user can have to > 3
- Self Provisioning IVR Directory Number > 8009400
- Starting auto-registration Directory Number > 8000001

- Ending auto-registration Directory Number > 8009000
- Select Check Line, Self-Provisioned Single Number Reach, IM and Presence, Voicemail, Extension Mobility Access, Extension Mobility Line, depending on the preferred services.
- Under Cisco Jabber Select check the kind of Cisco Jabber type from Cisco Jabber for BlackBerry, Desktop, Android, IPhone, and Tablet.
- Click **Save and Continue**.

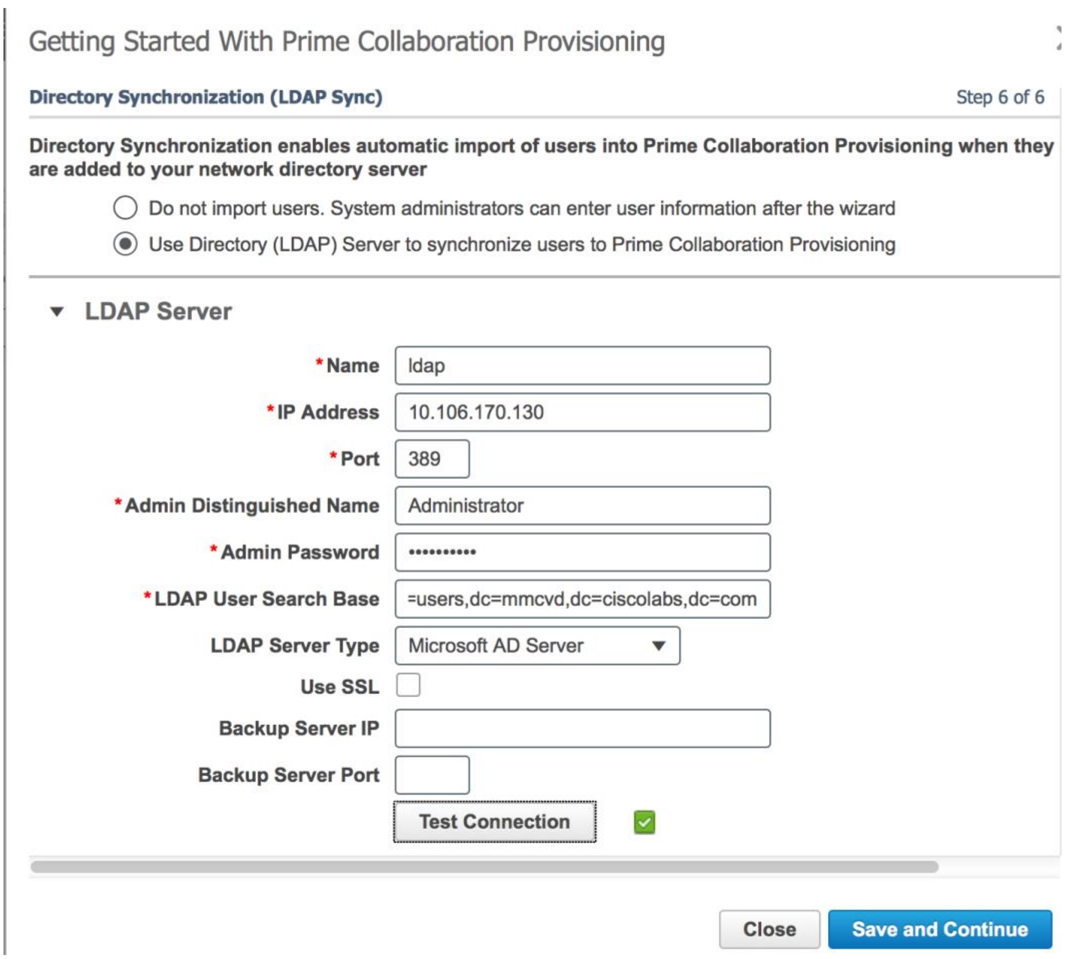


Step 11. Synchronize directory (LDAP Sync). Select Use Directory (LDAP) Server to synchronize users to Prime Collaboration Provisioning.

Under the LDAP Server pane, enter the following:

- Name > LDAP

- IP Address > 10.106.170.130
- Port > 389
- Admin Distinguished Name > Administrator
- Admin Password > **********
- LDAP User Search Base > cn=users,dc=mmcvd,dc=ciscolabs,dc=com
- LDAP Server Type > Microsoft AD Server
- Click **Test Connection**. It should have a green check mark. If not, verify the credentials again.



Step 12. Under the Sync policy settings, enter the following:

- Mode > Authentication and Synchronization
- Re-Sync Every > days > 1
- Users Search Base > cn=users,dc=mmcvd,dc=ciscolabs,dc=com

Step 13. Under Domain LDAP settings, enter the following:

- Filter Query for Synchronization > Synchronize all users

Step 14. Under Service Area LDAP settings, enter the following:

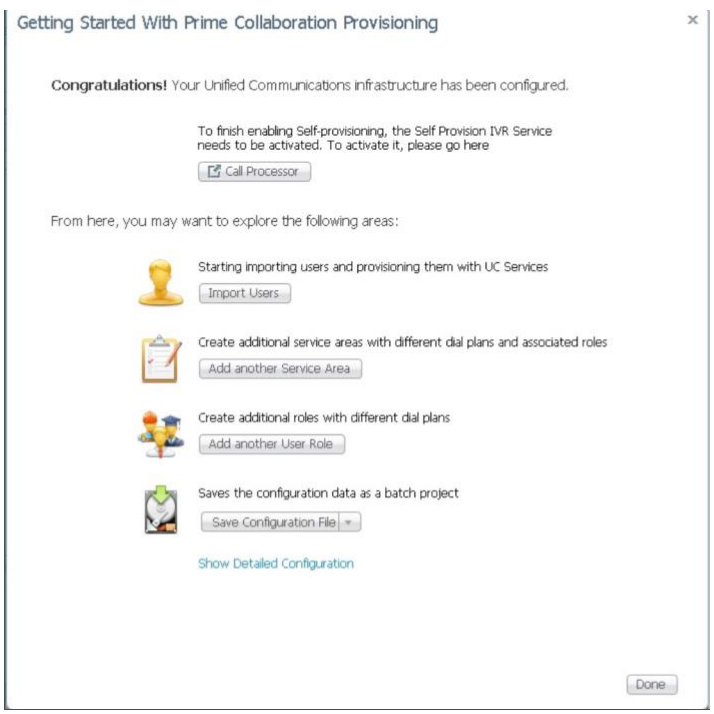
- Filter By > Title = Employee

Step 15. Under Line Settings, enter the following:

- Select **check Assign new line from the extension block**.
- Select **check Apply mask to LDAP synchronized telephone number**. Click **Save and Continue**.

Step 16. Under the Summary step, click Apply. The changes are applied in a few minutes.

Step 17. Click on **Import users**> select from **LDAP > Domain** : Main > Click **Import**. Complete the configuration, and then click **Done**.



Configuring Conference Bridges and SRST

PROCESS

1. Configure conference bridges
2. Configure SRST for phones
3. Block voice traffic on WAN links

The procedures in this process are required for all voice routers.

Please follow the steps in this process to understand what site-specific information is required in each section of the gateway template files.

Procedure 1 Configure Conference Bridges

All routers need a minimum of a packet voice digital signal processor (DSP) module (PVDM3) to create conference bridge resources along with the DSPs needed for voice gateway services. If your organization needs more gateways or conference resources, you will need additional DSPs. The router requires additional DSPs and configuration if hardware-based transcoding is needed. By default, calls to Cisco Unity Connection are transcoded in the application.

The router at the main site can provide unified communications gateway functions. Therefore, it should be configured with sufficient DSPs and a T1/E1 voice/WAN interface card (VWIC) for the PSTN primary rate interface (PRI) configurations.

The Cisco 4431 Integrated Services Routers ship with a PVDM4, so they have enough DSPs to handle one voice T1 and five 8-party conferences. If the remote site uses E1, they will have enough DSPs for only four 8-party conferences. The Cisco 4331 Integrated Services Router (ISR) ships with a PVDM4.

Apply the following configuration in the HQ router to register the five conference bridge resources as the highest priority on the primary subscriber and as the second priority on the backup subscriber. The same configuration is used in the remote site routers if conferencing resources are needed.

Step 1. Configure the DSP services on the voice card.

```
voice-card 0
  dspfarm
  dsp services dspfarm
```

Step 2. Configure the dspfarm profile for a conference bridge with a maximum of 5 sessions and a list of the acceptable codecs.

```
dspfarm profile 1 conference
  description HQ Conference Bridges
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec g729r8
  codec g729br8
  codec g722-64
  codec ilbc
maximum sessions 5
  associate application SCCP
  no shutdown
```

Step 3. Configure the interface used to register to the Cisco Unified CM. If you are adding voice configuration to an existing router, use the Loopback 0 interface.

```
ccm-manager sccp local loopback 0
```

If you are using a standalone voice router, use the interface connecting to the LAN.

```
ccm-manager sccp local [interface type][number]
```

Step 4. Configure the SCCP gateway interface to connect to the Cisco Unified CM servers used for subscription. If a large number of conference bridges are implemented, the priority of the subscriptions should be balanced appropriately by alternating the IP addresses of the Unified CM subscribers in the cluster. Set the version to 7.0 and above.

```
sccp local [interface type][number]
sccp ccm 10.106.170.136 identifier 1 priority 1 version 7.0
sccp ccm 10.106.170.135 identifier 2 priority 2 version 7.0
sccp
```

Step 5. Bind the interface for the conference bridge to the one used by the SCCP applications. Group the servers created in Step 4 and associate them with the profile for the conference bridge. Again, if a large number of conference bridges is implemented, the priority should be balanced appropriately. Register the conference bridge with Cisco Unified CM, set the switchback method to graceful, and then wait for 60 seconds.

```
sccp ccm group 1
  bind interface [interface type][number]
  associate ccm 1 priority 1
  associate ccm 2 priority 2
  associate profile 1 register CFB1HQ1
  switchback method graceful
```

```
switchback interval 60
```

i	Tech Tip
	The Cisco Unified CM configuration for the conference bridge was completed with PCP, so the registration name must match the name uploaded into the cluster by the tool. The names are always CFB1<Site Name> and CFB2<Site name>, if there are two. For example, if the headquarters site is HQ1, the conference bridge names are CFB1HQ1 and CFB2HQ1.

Procedure 2 Configure SRST for Phones

This procedure configures SRST for phones.

If sites codes are used for this installation, the dialplan-pattern command transforms the ten digit E164 PSTN number into the unique seven digit directory number on the phone. The extension-length and extension-pattern keywords enable you to identify the last four digits of the E164 number. You can create additional dial peers in order to maintain seven-digit dialing between sites with site codes.

For networks with 90 sites or less, the dial plan consists of the following:

- One digit as an inter-site access code
- Two digits for the site code to accommodate up to 90 sites
- Four digits for the site extension

The format is 8 + SS + XXXX, where 8 is the on-net access code, SS is a 2-digit site code from 10-99, and XXXX is a 4-digit extension number, giving a total of seven digits.

To allow the users to maintain 4-digit dialing between the phones at each remote site, a voice translation rule and profile are associated with incoming calls. The voice translation profile is active only when the phones are in SRST mode.

If sites codes are not used for this installation, the dialplan-pattern command transforms the 10-digit E164 PSTN number into the unique 4-digit directory number on the phone. The extension-length and extension-pattern keywords allow you to identify the last four digits of the E164 number. Voice translation rules and profiles are not needed for installations that do not use site codes.

Step 1. If site codes are used, create a voice translation rule and a voice translation profile in the global area of the router. The first part of the translation rule—between the first set of forward slashes—matches a four-digit number that starts with a 1 through 7. The second part of the rule—between the second set of forward slashes—prepends the unique site code to the four-digit dialed number. The translation profile called SRST-4-Digit applies the translation rule to the number called by the user. The example given is for seven-digit directory numbers starting with 820.

```
voice translation-rule 1
rule 1 /^[1-7]...$/ /811\0/

voice translation-profile SRST-4-Digit
translate called 1

voice translation-rule 800
 rule 2 /^800\(.*)//1310610\1/

voice translation-profile SRST-7-Digit
 translate called 800
```

Step 2. Create the SIP back-to-back user agent and SIP registrar functionality. Change the SIP registrar expiration timer to 600 seconds.

```
voice service voip
 allow-connections sip to sip
 sip
  registrar server expires max 600 min 60
```

Step 3. Assign the following characteristics to SIP phones globally: the system message on the bottom of certain phones, the maximum directory numbers, and the maximum number of pools allowed on the SRST router.

```
voice register global
 system message "SIP SRST Service"
 max-dn 200
 max-pool 50
```

i	Tech Tip
When the command max-pool 50 is executed, a license agreement appears. To activate this feature, you must accept the agreement. Be aware of this when copying and pasting or scripting the deployment of these features, as configuration cannot continue until this agreement is accepted.	

Step 4. If two-digit site codes are used for this installation, translate the inbound number to the seven-digit directory number for the phone. When a ten-digit call arrives from the PSTN carrier, the call is directed to the correct phone based on the access code, two-digit site code, and the last four digits. This configuration is done under call-manager-fallback

```
call-manager-fallback
 dialplan-pattern 1 311611.... extension-length 7
 extension-pattern 811....
```

If site codes are not used for this installation, configure the translated number to match the 4-digit directory number for the phone. When a 10-digit call arrives from the PSTN carrier, the call is directed to the correct phone based on the last four digits.

```
call-manager-fallback
  dialplan-pattern 1 311611.... extension-length 4 extension-
 pattern
  ....
```

Step 5. If site codes are used for this installation, add VoIP dial peers in order to maintain dialing between sites in SRST mode. The examples given are for the access code, 2-digit site codes, 7-digit directory numbers, and 10-digit outbound PSTN numbers.

Example: Headquarters Site

```
dial-peer voice 810 voip
 description 7-DIGIT DIAL to HQ in SRST
 translation-profile outgoing SRST-7-Digit
 destination-pattern 810....
 session protocol sipv2
 session target ipv4:10.106.170.136
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
```

Repeat this step for each additional remote site. Use an appropriate dial-peer number, description, destination pattern, and prefix.

Step 6. Configure the voice register pool for the defined IP address range. If your IP address ranges are not contiguous, you may create multiple pools. The id network is the IP subnet for the voice VLAN. Create a voice pool for each voice subnet implemented at the remote site. In this example, we are using two voice subnets. Use rtp-nte sip-notify for the dtmf-relay parameter, and use the G711 ulaw codec for all calls.

```
voice register pool  1
 id network 10.106.170.1 mask 255.255.255.0
 dtmf-relay rtp-nte sip-notify
 codec g711ulaw
```

Step 7. Identify the IP address of the Cisco Unified CM subscriber 1 and subscriber 2 as the external registrars, using the default expiration of 3600 seconds that is defined in the cluster.

```
sip-ua
 registrar ipv4:10.106.170.136 expires 3600
 registrar ipv4:10.106.170.135 expires 3600 secondary
```

Procedure 3 Block Voice Traffic on WAN links

(Optional)

In some cases, an administrator may want to force IP phones into SRST mode when a failover to a backup WAN link occurs. Implementing this blocking avoids transmitting voice over a lossy link, and it decreases the cost of a failure by reducing data usage while maintaining the dial tone that end-users expect. This configuration can be applied to the backup router of a dual router design or to the secondary link of a single router design. This configuration can also be used on any WAN interface when centralized voice registrations are not wanted at a particular remote site.

Tech Tip

The Cisco IOS commands are listed under the Optional - Block Voice on WAN section in the template file for each voice gateway.

The hardware-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to understand what is needed in each area of the configuration.

Step 1. Configure the access list that blocks SIP: 5060 (TCP/UDP), Secure SIP: 5061 (TCP/UDP), SCCP: 2000 (TCP), Secure SCCP: 2443 (TCP), standard RTP ports: 16384-32767 (UDP), and allow all other traffic.

```
ip access-list extended ACL-VOIP-CONTROL
 deny tcp any any eq 5060
 deny udp any any eq 5060
 deny tcp any any eq 5061
 deny udp any any eq 5061
 deny tcp any any eq 2000
 deny tcp any any eq 2443
 deny udp any any range 16384 32767
 permit ip any any
```

Step 2. Apply the access control list to the WAN interface to which the administrator wants to block voice traffic.

```
interface Tunnel10
 ip access-group ACL-VOIP-CONTROL in
 ip access-group ACL-VOIP-CONTROL out
```

Appendix A: Product List

Data Center or Server Room

Component	Product Description	Part Numbers	Software
Call Control	Cisco Business Edition 6000 with up to 1000 users	BE6M-M5-K9	12.0.1.1.22900-12
Unity Connection	Cisco Business Edition 6000 with up to 1000 users		12.0.1.1.22900-14
IM & Presence	Cisco Business Edition 6000 with up to 1000 users		12.0.1.10000-12
Prime Collaboration	Cisco Business Edition 6000 with up to 1000 users		12.5.0.1862-small.ova

Headquarters Voice

Functional Area	Product Description	Part Numbers	Software
Headquarters Voice Router	Cisco ONE ISR 4431 (4GE, 3NIM, 1 ISC, 8G FLASH, 4G DRAM,)	C1-CISCO4431/K9	16.9.1 ED
	2-port multi-flex trunk voice/channelized data T1/E1 Module.	NIM-2CE1T1-PRI	
	2-port clear channel data and voice T1/E1 module.	NIM-2MFT-T1/E1	

Site Voice

Functional Area	Product Description	Part Numbers	Software
Remote Site Voice Router	Cisco ONE ISR 4321 (2GE, 2NIM, 4G Flash, 4G DRAM, IPB)	C1-CISC04321/K9	16.9.1ED
	2-port multi-flex trunk voice/channelized data T1/E1 Module.	NIM-2CE1T1-PRI	
	2-port clear channel data and voice T1/E1 module.	NIM-2MFT-T1/E1	

Endpoints

Functional Area	Product Description	Part Numbers	Software
Phones	Unified IP Phone 7800 Series	CP-7821-K9 CP-7841-K9 CP-7861-K9	78xx.12-1.12
	Unified IP Phones 8800	CP-8841-K9= CP-8851-K9=	88xx.12-1.ISR1
Soft Client	Jabber	Cisco Jabber for Windows	Jabber_for_Windows-12.1(0)
Soft Client	Jabber	Cisco Jabber for Mac	Jabber_for_Mac-12.1(0)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**